UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

LEONARD LICHT, ZHENGJUN CAI, HENRY CHEN, DANIEL CHANG, DOMINIC CHOW, CHENGGUO DONG, AMINE FENNANE, IHAB W. FRANCIS, JOHN GORDON, SHAI GRANOVSKI, DALTON GREEN, MICHAEL GRILLI, IRAKLIS KARABASSIS, ALICIA LAU, TREVOR LAU, NADER LOBANDI, EISI MOLLANJI, JAMES MOSKWA, ANH NGUYEN, BRIAN ROTHAUS, GORDON SHAYLOR, RICHARD SLAVANT, NATHANIAL THRAILKILL, JACK YAO, EDMUND YEO, and JUN ZHAI,

Plaintiffs,

v.

BINANCE HOLDINGS LIMITED, d/b/a BINANCE.COM, BAM TRADING SERVICES, INC., d/b/a BINANCE.US, and CHANGPENG ZHAO,

Defendants.

No. 24-cv-10447

JURY DEMANDED ON ALL CAUSES OF ACTIONS

FIRST AMENDED COMPLAINT

Lead plaintiff Leonard Licht and the 25 additional Plaintiffs identified herein bring this amended complaint against Defendants Binance Holdings Limited ("Binance"), BAM Trading Services, Inc. ("BAM"), and Changpeng Zhao ("Zhao") pursuant to the federal civil Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1964(c).

I. INTRODUCTION

1. Binance is a Cayman Islands corporation that operates the world's largest cryptocurrency exchange, Binance.com. Binance was founded by Changpeng Zhao. Zhao

maintained majority ownership of Binance and served as its CEO until November 2023, amassing a fortune that made him the 69th richest person in the world, according to Forbes Magazine. For years, however, Binance and Zhao knowingly and willfully operated the Binance exchange in flagrant violation of United States criminal statutes, including anti-money laundering statutes and statutes prohibiting unlicensed money transmitting businesses.

2. Binance profited handsomely from its crimes, but federal prosecutors eventually caught on to Binance's schemes. On November 21, 2023, Binance and Zhao pled guilty, in the United States District Court for the Western District of Washington, to several federal crimes, including (1) conspiracy to violate the anti-money laundering requirements of the federal Bank Secrecy Act, 31 U.S.C. §§ 5318(h) and 5322; and (2) conspiracy to conduct an unlicensed money transmitting business, 18 U.S.C. §§ 1960(a) and 1960(b)(1)(B). *See United States of America v. Binance Holdings Ltd.*, No. 23-cr-178, Dkt. #21; *United States of America v. Changpeng Zhao*, No. 23-cr-179, Dkt. #29. Binance's plea agreement requires it to pay a criminal fine of more than $1.8 billion and criminal forfeiture of more than $2.5 billion, and on April 30, 2024, Zhao was sentenced to a term of imprisonment of four months and ordered to pay a criminal fine of $50 million as a consequence of his plea.

3. As Judge Jones explained at Zhao's sentencing, "I was deeply trouble . . . by [Zhao's] statement . . . that it was better to ask for forgiveness than permission."[1] The Judge further described Zhao's and Binance's crimes as "unprecedented in terms of volume, scale and massiveness in dollar impact of noncompliance."[2] Shockingly, and straining all credulity, Zhao's

[1] *See* https://www.theverge.com/2024/4/30/24145689/i-was-deeply-troubled-by-your-statement-reflected-on-pg-1-the-opening-line-of-the-governments-brief

[2] https://www.theverge.com/2024/4/30/24144807/binance-founders-sentencing-hearing-liveblog

defense attorneys consistently referred to Zhao's conduct as a "mistake."[3] But it was not a "mistake"—it was purposeful, intentional conduct that was documented in thousands of contemporaneous business records showing that Binance's business model, as orchestrated and directed by Zhao, was predicated on facilitating criminal activity around the globe, including the pig butchering schemes that ensnared the Plaintiffs. In any event, none of those fines or forfeiture, or even Zhao's request for "forgiveness," will provide solace, let alone compensation, to the flesh and blood victims of Binance's and Zhao's crimes, whose lives have been shattered as a direct result of the Defendants' actions.

4. Binance's and Zhao's crimes were not victimless regulatory infractions. To the contrary, Binance's and Zhao's systematic criminal conduct—conduct that defendant BAM also participated in and conspired with—enabled criminal syndicates to ensnare innocent, vulnerable victims into financially devastating cryptocurrency fraud schemes, including one type of predatory scheme known as "pig butchering." Binance and Zhao knowingly and willfully allowed the criminal syndicates to use the Binance.com exchange to launder their criminal proceeds and to convert those proceeds into untraceable, unrecoverable fiat currency, and BAM participated in and conspired with those racketeering acts as well. In short, Binance and Zhao, with BAM's participation and assistance, knowingly and willfully provided the figurative "getaway car." Binance did so for a very simple reason: money. Binance received lucrative fees on every transaction that the criminal syndicates conducted on the Binance exchange, which amounted to hundreds of millions of dollars in illicit profits for Binance.

[3] https://www.theverge.com/2024/4/30/24144807/binance-founders-sentencing-hearing-liveblog

5. This complaint is brought by 26 of Binance's, Zhao's, and BAM's innocent victims of Zhao and Binance's "mistake." The Plaintiffs are hardworking, ordinary people who lost significant sums of money—in some instances, life-changing sums of money—in illicit pig butchering schemes that utilized and were accomplished through the Binance exchange and that were facilitated by the Defendants' systematic, prolonged, and willful violations of federal criminal laws that Congress rightfully has declared to be RICO predicate acts.

6. One Plaintiff, Lenny Licht was bilked out of almost $3 million. Once he realized that he had been defrauded, he sought to recover the cryptocurrency that he had sent to a supposed cryptocurrency investment fund that in fact was a fraud scheme. This included retaining a blockchain investigation firm called CipherBlade and working with a criminal investigator from the United States Secret Service. If Lenny's cryptocurrency had remained in the self-custodied wallet to which Lenny unwittingly had sent it, that cryptocurrency would have been fully recoverable by federal law enforcement. But it had not. The criminal syndicate laundered the criminal proceeds through Binance's exchange, specifically by transferring Lenny's cryptocurrency from the self-custodied wallet to multiple accounts on Binance's exchange. This enabled the criminal syndicate to vanish into thin air with Lenny's hard-earned money.

7. If Binance had been operating in compliance with United States laws, it would have identified that the criminal syndicate that scammed Lenny was using Binance for illicit purposes and frozen the syndicate's Binance wallets, which in turn would have enabled United States law enforcement to seize the stolen cryptocurrency and return it to Lenny and the other Plaintiffs here. But Binance was not complying with United States laws. Binance and Zhao knew that criminal syndicates, such as the syndicate that defrauded Lenny, were using the Binance exchange in this manner to effectuate their frauds. Binance and Zhao knew that they were facilitating those criminal

syndicates' activities. Binance and Zhao knew that Binance could put a stop to the criminal syndicates' activities, including by freezing Binance accounts that were being utilized for suspicious transactions and reporting those transactions to FinCEN. Binance also knew that its conduct was itself a violation of federal criminal laws. But Binance did not care. Binance cared more about the lucrative fees that it earned on every transaction that occurred on the Binance exchange, including money laundering transactions that enabled the criminal syndicates to get away with their fraud schemes. It also cared about avoiding compliance with United States laws, including FinCEN registration requirements and anti-money laundering statutes, which might impair Binance's singular obsession with gaining market share. In Zhao's own words, Binance had to "do everything to increase our market share, and nothing else."

8. Lenny Licht's story is unfortunately not unique. Binance's systematic, willful violations of federal criminal laws designed to keep financial markets safe and free from money laundering led to the exact result that Binance's own employees and executives—including Zhao—knew and predicted would result: criminal syndicates from around the world constructed fraud schemes that would and did use the Binance exchange as their proverbial getaway cars, stealing massive amounts of money from thousands of people. Lenny Licht's co-Plaintiffs in this amended complaint are among the Defendants' victims, and their stories are summarized herein.

9. It is now time for Binance, BAM, and Zhao to take responsibility, and to be held liable, for the devastating financial harm that their flagrantly unlawful racketeering activity caused to Plaintiffs.

II. THE PARTIES

10. Plaintiff Leonard Licht ("Lenny") is a United States citizen who resides in Plano, Texas.

11. Plaintiff Zhengjun Cai is a Chinese citizen who resides in Irvine, California.

12. Plaintiff Henry Chen is a United States citizen who resides in San Francisco, California.

13. Plaintiff Daniel Chang is a United States citizen who resides in San Jose, California.

14. Plaintiff Dominic Chow is a United States citizen who resides in Lexington, Massachusetts.

15. Plaintiff Chengguo Dong is a United States citizen who resides in Fremont, California.

16. Plaintiff Amine Fennane is a citizen of France who resides in Paris, France.

17. Plaintiff Ihab W. Francis is United States citizen who resides in New City, New York.

18. Plaintiff John Gordon is a United States citizen who resides in Miami, Florida.

19. Plaintiff Shai Granovski is a Canadian citizen who resides in North York, Ontario, Canada.

20. Plaintiff Dalton Green is a United States citizen who resides in Colorado Springs, Colorado.

21. Plaintiff Michael Grilli is a United States citizen who resides in Palm Beach Gardens, Florida.

22. Plaintiff Iraklis Karabassis is a United States citizen who resides in Miami, Florida.

23. Plaintiff Alicia Lau (Lau Pui Mei) is a citizen of Malaysia who resides in Singapore.

24. Plaintiff Trevor Lau is a Canadian citizen who resides in Ontario, Canada.

25. Plaintiff Nader Lobandi is a citizen of Iran who resides in Boston, Massachusetts.

26. Plaintiff Eisi Mollanji is a Canadian citizen who resides in Manitoba, Canada.

27. Plaintiff James Moskwa is a United States citizen who resides in Coventry, Rhode Island.

28. Plaintiff Anh Nguyen is a United States citizen who resides in Anaheim, California.

29. Plaintiff Brian Rothaus is a United States citizen who resides in Elkins Park, Pennsylvania.

30. Plaintiff Gordon Shaylor is a United States citizen who resides in Henderson, Nevada.

31. Plaintiff Richard Slavant is a United States citizen who resides in Monroe, Louisiana.

32. Plaintiff Nathanial Thrailkill is a United States citizen who resides in Litchfield Park, Arizona.

33. Plaintiff Jack Yao is a United States citizen who resides in San Diego, California.

34. Plaintiff Edmund Yeo (Yeo Yin Pin Edmund) is a citizen and resident of Singapore.

35. Plaintiff Jun Zhai is a United States citizen who resides in Seattle, Washington.

36. Defendant Binance Holdings Limited ("Binance") is a Cayman Islands company founded in or around 2017. Binance previously has touted itself as being essentially "headquarterless." Its founder and former CEO Changpeng Zhao stated in 2020, "Wherever I sit, is going to be the Binance office." In its November 2023 plea agreement, Binance admitted that, at least through October 2022, it "did business wholly or in substantial part within the United States." Binance also admitted that more Binance customers resided in the United States ***than any other country***, notwithstanding Binance's false public representations that United States customers exclusively utilized BAM's Binance.US platform and were blocked from using the Binance exchange.

37. Defendant BAM Trading Services, Inc. ("BAM") is a Delaware corporation headquartered either in Florida or Palo Alto, California. Doing business as Binance.US, BAM continuously and systematically transacts business throughout the United States, including in the District of Massachusetts. BAM is not a subsidiary of Binance, nor does BAM operate under a unified corporate structure with Binance. Indeed, in prior federal court actions, Binance and BAM have represented that BAM is not even a corporate *affiliate* of Binance.

38. Defendant Zhao is a Chinese-born citizen of Canada. Zhao is the founder and former CEO of Binance. Until at least 2022, Zhao owned approximately 90% of Binance's equity and BAM's equity and directed and controlled all of Binance's and BAM's corporate decisions, strategies, and conduct. Although Zhao is presently living somewhere in the continental United States by court order, pending his criminal sentencing for violations of the Bank Secrecy Act, the United States is not where Zhao is "domiciled." On information and belief, Zhao's domicile is Dubai.

III. JURISDICTION AND VENUE

39. This court has subject matter jurisdiction pursuant to 18 U.S.C. § 1964(a) (RICO jurisdiction) and 28 U.S.C. § 1331 (federal question jurisdiction).

40. This court has general personal jurisdiction over Binance because, as Binance admitted in the Statement of Facts accompanying its November 2023 criminal plea, Binance "did business wholly or in substantial part within the United States" during the period 2017 through "at least October 2022." *See, e.g.*, *Perkins v. Benguet Consolidated Mining Co.*, 342 U.S. 437 (1952); *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408 (1984); *Northeast Structures, Inc. v. Wolfeboro Corinthian Yacht Club, Inc.*, 138 F.R.D. 345, 347 (D.R.I. 1991) ("A foreign corporation defendant may be subjected to the forum state's reach if its activities are 'substantial'

or 'continuous and systematic [in the forum state],' even if these activities do not relate to the cause of action."); *see also Omni Video Games, Inc. v. Wing Co. Ltd.*, 754 F. Supp. 261, 263 (D. R.I. 1991) (holding that because the civil RICO statute provides for nationwide service of process, the defendant needs only to have had sufficient contacts with the United States for personal jurisdiction to apply). General personal jurisdiction over Binance is also warranted because at least until the end of 2022, at Zhao's express direction, Binance clandestinely maintained custody and control of the cryptocurrency assets that deposited, held, and traded on BAM's Binance.US platform, and maintained extensive ties to the operation of the Binance.US platform. General personal jurisdiction over Binance is also warranted because the Binance.com exchange was, during the relevant time period, maintained on Amazon Web Services ("AWS") servers located in the State of Washington, and those servers acted as Binance's figurative heart—as the Commodities Futures Trading Commission put it, "No AWS servers, no Binance exchange." In addition, a FinCEN investigation found that Binance "maintained U.S.-based personnel and other operational touchpoints to the United States" during the time period relevant to this complaint. FinCEN found that Binance employed "more than 100 individuals who are based in the United States, including senior personnel, such as an advisor to [Zhao], several C-suite executives (e.g., the former Chief Business Officer, former Chief Strategy Officer, Chief Technology Officer), Global Director of Brand Marketing, and Vice President of Global Expansion Operations." FinCEN also found that Binance's most substantial market makers—that is, the persons and entities providing the daily trading liquidity that Binance needed for the Binance exchange to operate successfully—were based in the United States. Binance's unlawful U.S. operations included regularly and continuously soliciting and doing business with customers located in the

Commonwealth of Massachusetts, including on information and belief Commonwealth-based market makers.

41. This court also has specific personal jurisdiction over Binance because the racketeering acts that are the predicates for the RICO causes of action against Binance include (1) Binance's purposeful availment of the United States cryptocurrency trading market, without registering with FinCEN as a money transmitting business, in violation of 18 U.S.C. § 1960(a), which also had the effect of making every transaction on the Binance exchange a violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross reference to 18 U.S.C § 1961(1) (defining "racketeering activity" to include violations of 18 USC § 1960); (2) Binance's formation of a RICO enterprise with BAM, a Delaware corporation headquartered in Florida or California, whose common purpose was to deceive United States law enforcement regarding Binance's connections to and exploitation of the United States market; (3) Binance instructing U.S.-based "VIP users" on how to use the Binance exchange while concealing their United States location, in furtherance of the Binance/BAM enterprise's racketeering activity; (4) Binance's secret (and unlawful) solicitation, recruitment, and retention of U.S.-based "market makers," including high-frequency quantitative trading firms, that provided the Binance exchange with the substantial, sought-after liquidity that attracted criminal syndicates who needed a highly liquid laundering facility and cash-out point for their stolen cryptocurrency assets; (5) Binance's participation in the laundering of the cryptocurrency assets that criminal syndicates stole from Plaintiffs, many of them United States citizens, by means of fraudulent representations; and (6) Binance's solicitation of U.S.-based "market makers" that provided the daily trading liquidity that served as the means by which money laundering schemes on the Binance exchange succeeded. Binance's unlawful U.S. operations including regularly and continuously soliciting and doing

business with customers located in the Commonwealth of Massachusetts, including on information and belief Commonwealth-based market makers.

42. This court has general personal jurisdiction over BAM because RICO provides for nationwide service of process and BAM conducts all or substantially all of its business in the United States, is incorporated in Delaware, and is headquartered in Florida or California. This court also has specific personal jurisdiction over BAM because, as part of its role in concealing (and therefore facilitating) Binance's and Zhao's criminal conduct and deceiving U.S. regulators and law enforcement, BAM conducted substantial and continuous business operations in the Commonwealth, including regularly and continuously soliciting and doing business with customers based in the Commonwealth.

43. This court has general personal jurisdiction over Zhao because, as the CEO, control person, and approximately 90% equity holder of Binance during the relevant time period, as well as the Chairman of the Board of Directors and approximately 90% equity holder of BAM during the relevant time period, Zhao had continuous and systematic business contacts with the United States market that substantially enriched him personally.

44. This court also has specific personal jurisdiction over Zhao because (1) he participated in and directed the conduct of the various RICO enterprises' predicate racketeering acts that were specifically directed at the United States market (namely, the 18 U.S.C. 1960(a) violations), including by directing BAM's U.S.-based business operations and BAM's U.S.-based deceptions of United States regulators and law enforcement; and (2) he conspired in the laundering on the Binance exchange of cryptocurrency assets stolen from U.S. citizen plaintiffs by criminal syndicates by means of false representations sent via international wire communications.

45. Venue is proper in this judicial district under the RICO statute's venue provisions, 18 U.S.C. § 1965(a)-(b). First, BAM operates a U.S.-based crypto exchange whose nationwide operations include regularly and continuously soliciting, providing substantial services to, and profiting substantially from Massachusetts-based customers. BAM has registered with the Massachusetts Secretary of State's Office, stating that it operates a "Digital Asset Marketplace" in the Commonwealth; BAM also has designated registered agents in the Commonwealth. Second, as the SEC found after its lengthy investigation of Binance and Zhao, Binance and Zhao effectively "controlled" and were "integrally involved in" all of BAM's business operations, including its business operations in Massachusetts. Because Zhao owned virtually all of Binance's equity, and because Binance owned essentially all of BAM's equity, BAM's regular, substantial, and continuous business transactions in the United States, including all the business transactions that occurred in and exploited the market in Massachusetts, were effectively Binance's and Zhao's. Third, a substantial portion of Binance's systematic, unlawful U.S.-based operations—operations that it hid from United States regulators and law enforcement—occurred in or exploited the Massachusetts market, including regularly and continuously soliciting and providing services to Massachusetts-based customers and facilitating and settling cryptocurrency trades of Massachusetts customers. Binance's regular, substantial, and continuous business transactions in the Commonwealth essentially were the business transactions of Zhao, given that Zhao owned virtually all of Binance's equity and directed and tightly controlled Binance's decisions. Accordingly, 18 U.S.C. § 1965(a) vests this Court with venue over each of the Defendants. Furthermore, to the extent 18 U.S.C. § 1965(a) vests this Court with venue over some but not all of the Defendants, the Court would be permitted to exercise venue over the remaining Defendants

pursuant to 18 U.S.C. § 1965(b) in the interests of justice, particularly given that Binance and Zhao already "may be sued in any judicial district" pursuant to 28 U.S.C. § 1391(c)(3).

IV. FACTUAL ALLEGATIONS

A. Binance's and Zhao's Admitted Violations of United States Criminal Law[4]

46. Starting at least as early as August 2017 and continuing until at least October 2022, Binance—led by its founder, owner, and CEO Changpeng Zhao, and certain of its officers, directors, employees, and agents—knowingly failed to register with FinCEN as a money transmitting business, in violation of 18 U.S.C. § 1960, and willfully violated the Bank Secrecy Act by failing to implement and maintain an effective anti-money laundering program.

47. Binance's violations of federal criminal law were part of a deliberate and calculated effort to profit from the United States cryptocurrency market without implementing controls required by United States law.

48. During the August 2017 through October 2022 period, Binance operated wholly or in substantial part in the United States by serving a large number of United States users. Because of the nature of the Binance exchange, Binance was operating an unlicensed money transmitting business in violation of United States law. Binance operated as an unlicensed money transmitting business in part to prevent United States regulators from discovering that Binance was facilitating

[4] Nearly every allegation in this subsection of the complaint is a verbatim or near-verbatim copy of the respective Statements of Facts appended to Binance's and Zhao's November 2023 plea agreements. Having agreed to the Statements of Facts as part of their pleas, Binance and Zhao should be precluded from collaterally challenging the factual allegations in this subsection of the complaint, at least insofar as the factual allegations track those in the plea agreements' Statements of Facts. *See, e.g., Trinidad v. City of Boston*, No. 07-CV-011679-DPW, 2010 U.S. Dist. LEXIS 71900, at *22 (D. Mass. July 16, 2010) ("Federal Courts of Appeals, including the First Circuit, applying federal law, have accorded preclusive effect to federal guilty pleas in [ ] subsequent federal civil proceedings.").

billions of dollars of cryptocurrency transactions on behalf of its customers without implementing appropriate "know your customer" procedures or conducting adequate transaction monitoring.

49. Due to Binance's willful failure to implement an effective anti-money laundering program, Binance processed transactions by users who operated illicit mixing services and were laundering proceeds of darknet market transactions, hacks, ransomware, and scams (including pig butchering scams).

50. Binance users could store and trade value in the form of virtual assets, including cryptocurrency, in accounts (or "wallets") maintained by Binance. When a user opened a Binance account, Binance assigned them a custodial virtual currency wallet—*i.e.*, a wallet in Binance's custody that allowed the user to conduct transactions on the platform, including transferring funds to other Binance users or accounts or to external virtual currency wallets, and to convert cryptocurrency into fiat currency that could then be transferred into traditional bank accounts (including accounts at wholly foreign banks outside the purview of United States regulatory authorities) or otherwise withdrawn.

51. Binance charged its users fees on every transaction that the users conducted on Binance. Binance thus had an economic incentive to allow, and profited from allowing, illicit transactions on the Binance exchange. Binance chose not to comply with United States legal and regulatory requirements, including anti-money laundering requirements, because it determined that doing so would limit the scale and speed of its revenue growth.

52. Because Binance was operating a money transmitting business, it was required to register with FinCEN, or risk criminal penalties under 18 U.S.C. § 1960. Binance knew it was operating a money transmitting business required to be registered with FinCEN under 18 U.S.C. § 1960(a). Binance, however, chose not to register with FinCEN, meaning that it was willfully

operating in violation of 18 U.S.C. § 1960(a) every single day until at least October 2022. Because Binance was in violation of 18 U.S.C. § 1960(a), every transaction that Binance conducted on the Binance exchange during the relevant time period—which is to say, every transaction that occurred on the Binance exchange during the relevant time period—constituted a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1).

53. Binance also failed to comply with the Bank Secrecy Act's anti-money laundering provisions, which applied to Binance because it was operating a money transmitting business. The anti-money laundering provisions that Binance flouted included provisions designed to prevent a money transmitting business from being used to facilitate money laundering and the financing of terrorist activities, as well as provisions requiring the filing of suspicious activity reports with FinCEN and monitoring for suspicious transactions. Binance and Zhao knowingly and willfully did not systematically monitor transactions on Binance's exchange, as required by the Bank Secrecy Act's anti-money laundering provisions.

54. Binance and Zhao knew that, by not monitoring for suspicious transactions and not conducting "Know Your Customer" diligence as required by the Bank Secrecy Act, they were facilitating criminal activity. A Binance executive wrote to a colleague that Binance should create "a banner" stating, "[I]s washing drug money too hard these days[?] [C]ome to binance[,] we got cake for you." This was an acknowledgment that Binance was tacitly conspiring with criminals whom Binance and Zhao knew, or consciously avoided learning, were utilizing the Binance cryptocurrency exchange as a laundering facility and cash-out point for ill-gotten proceeds stolen from fraud victims.

55. Due to Binance's failure to implement an effective anti-money laundering program, illicit actors used Binance's exchange in various illicit ways, including: operating mixing services

that obfuscated the source and ownership of cryptocurrency; transacting illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams including pig butchering schemes. For example, between August 2017 and April 2022, there were direct transfers of approximately $106 million in bitcoin to Binance.com wallets from Hydra, a popular Russian darknet marketplace frequently utilized by criminals that facilitated the sale of illegal goods and services. These transfers occurred over time to a relatively small number of unique addresses, which indicates "cash out" activity by a repeat Hydra user, such as a vendor selling illicit goods or services. Similarly, from February 2018 to May 2019, Binance processed more than $275 million in deposits and more than $273 million in withdrawals from BestMixer, which was one of the largest cryptocurrency mixers in the world until it was shut down by Dutch authorities in May 2019. The forensics firm Chainalysis, which the United States government routinely hires to track illegal cryptocurrency transaction flow, concluded in a 2020 report that in 2019 alone the Binance exchange was used as a laundering facility for $770 million in illicit funds. A Reuters investigation found that from 2017 to 2021 Binance processed transactions totaling at least $2.35 billion stemming from hacks, investment frauds, and illegal drug sales.

56. Binance and Zhao knew that some of these "VIP users"—a term Binance used for customers who conducted substantial transaction volumes on the Binance exchange—were illicit actors or "high-risk users." In some instances, Binance and Zhao knowingly and willfully chose not to take any adverse action against such users' accounts, instead allowing these bad actors to continue to access and utilize the Binance exchange. In other instances, Binance engaged in sham compliance efforts, "shutting down" the users' accounts but then immediately allowing the users

to open up new accounts and, incredibly, providing those users instructions on how to avoid raising red flags with their future transactions.

57. To conceal its failure to comply with United States anti-money laundering requirements, and to conceal that it was operating an illegal money transmitting business without registering with FinCEN, Binance and Zhao formed in or around June 2019 a new entity that they publicly called Binance.US. Binance.US was the d/b/a identity of a Delaware corporation called BAM Trading Services, which was at least 90% owned by Zhao. In or around June 2019, Binance.US registered itself with FinCEN as a money transmitting business and made at least superficial efforts to comply with the Bank Secrecy Act's anti-money laundering provisions. Binance touted Binance.US as the cryptocurrency exchange to which U.S.-based customers would be directed. Binance did this, however, specifically and willfully to create a false and misleading impression that Binance itself was not servicing U.S.-based customers and, therefore, was not subject to United States laws including the Bank Secrecy Act. Binance, BAM, and Zhao knew, however, that the Binance.com exchange—which remained unregistered with FinCEN and was not attempting to comply (let alone actually complying) with the Bank Secrecy Act's anti-money laundering provisions—maintained a substantial United States user base.

58. Binance's founder and CEO Zhao created and launched Binance.US because he knew that the Binance.US entity, indirectly controlled by Binance, would become the focus of United States law enforcement and regulatory authorities, which would allow Binance itself to continue to profit from the United States market without actually complying with United States laws. In other words, Binance.US was, at least in part, created to provide a legal and regulatory smokescreen that would distract United States regulatory and law enforcement authorities from Binance itself. In Zhao's own words, the "goal" behind Binance.US was "to make the U.S.

regulatory authorities not trouble us." BAM conspired with Zhao's and Binance's plan to use Binance.US as a smokescreen that would enable Binance to continue to flout 18 U.S.C. § 1960(a) and the Bank Secrecy Act without drawing scrutiny from United States regulators and law enforcement. At least through October 2022, BAM agreed to, and did, falsely represent to the public, United States regulators, and United States law enforcement that all U.S.-based customers were being routed to the Binance.US exchange and were prohibited from utilizing the Binance exchange.

59. Binance and Zhao knew that, so long as Binance continued to have substantial business connections with the United States, Binance would be required to comply with United States registration requirements and the Bank Secrecy Act, notwithstanding the existence of Binance.US.

60. Binance and Zhao knew that its high-volume "VIP users"—which included VIP users whom Binance and Zhao knew, or consciously avoided learning, were engaged in illicit activities and using the Binance exchange to launder criminal proceeds—accounted for approximately 70% of the company's transaction revenues, and it knew that approximately 30% of those VIP users were based in the United States. After launching Binance.US, Binance executives and senior leaders, including CEO Zhao, encouraged these VIP users—including the VIP users based in the United States—to continue to utilize the Binance exchange (rather than Binance.US) and to conceal and obfuscate their United States connections. During a conference call on or around June 25, 2019, Binance employees and executives told CEO Zhao that they were contacting United States VIP users "offline" through direct phone calls so that Binance would "leave no trace." A Binance executive acknowledged that Binance's plan to retain its VIP users on the Binance platform was an "international circumvention of [Know Your Customer] rules."

Nevertheless, Binance continued to take steps in furtherance of that plan, including using a "script" that Binance representatives would use with VIP users that Binance and Zhao knew were based in the United States. The script included instructions to the VIP user on how the user could conceal his United States location by, among other things, altering the IP address of the computer that the user used to log in to Binance.com.

61. Approximately one year after Binance.US launched, Binance and Zhao knew that approximately 16% of Binance.com customers were based in the United States—***more than any other country***. In October 2020, Binance executives altered internal company reports to conceal this fact. Specifically, whereas company reports before October 2020 specifically identified the percentage of Binance.com customers who were based in the United States, beginning in October 2020, those same reports recategorized U.S.-based customers with the label "UNKWN."

62. According to Binance's own transaction data, United States users conducted trillions of dollars in transactions on the Binance.com exchange between August 2017 and October 2022—transactions that generated approximately $1.6 billion in transaction fees (pure profit) for Binance.

63. By concealing that the Binance.com exchange was serving a substantial percentage of U.S.-based customers, Binance illegally avoided registering with FinCEN and thereby illegally avoided complying with the Bank Secrecy Act's anti-money laundering requirements. Had Binance complied with those federal laws, Binance would have been required to conduct "Know Your Customer" diligence on *all* Binance.com customers—not just those customers based in the United States. It also would have been required to monitor the Binance.com platform for suspicious transactions and to notify FinCEN of suspicious transactions. Binance did none of these things, because it knew that being hospitable and attractive to illicit actors and eschewing anti-

money laundering obligations increased the size of Binance's customer base, increased Binance's transaction volume, and therefore enhanced Binance's profits and Zhao's personal fortune. Indeed, Binance *never* filed a suspicious activity report with FinCEN, despite knowing, consciously avoiding learning, and making themselves willfully blind to the fact that criminal syndicates were using the Binance exchange to facilitate their criminal schemes, specifically by using the Binance cryptocurrency exchange to launder stolen cryptocurrency assets and convert those stolen assets into fiat currency. According to FinCEN's investigatory findings, Binance's former Chief Compliance Officer reported to other Binance personnel that the senior management policy was to never report any suspicious transactions. Indeed, FinCEN found during its investigation that Binance elected to allow customers to continue to use the Binance exchange for transactions that a senior Binance manager described as "standard money laundering."

64. Binance, through its conduct and willful inaction, knowingly and willfully facilitated and at least indirectly participated in the fraud schemes that utilized the Binance cryptocurrency exchange as a laundering facility and cash-out point. Moreover, to the extent Binance and Zhao knew, consciously avoided learning, or made themselves willfully blind to the fact that certain of its customers were engaged in illicit money laundering on the Binance cryptocurrency exchange, Binance itself knowingly engaged in financial transactions in violation of 18 U.S.C. § 1956(a)(1)(A)-(B), because any financial transaction conducted through a Binance account by definition was a transaction involving Binance.

65. As early as September 2018, Binance executives acknowledged that Binance had "[n]othing . . . in place" to review high-volume accounts for suspicious activity and that many transactions were occurring on Binance.com that "in [the] aml [anti-money laundering] world" would be flagged for money laundering risks. Binance's CEO Zhao, however, said that he did

"see a need to" comply with anti-money laundering rules and that it was "better to ask for forgiveness than permission." CEO Zhao, and therefore Binance, believed that subjecting Binance's customers to a "Know Your Customer" process compliant with United States law, monitoring transactions for suspicious activity as required by the Bank Secrecy Act, and reporting suspicious transactions to FinCEN as required by the Bank Secrecy Act, would mean that some customers would choose not to use Binance and that others would be rejected or flagged by the compliance process, both of which would interfere with Binance's efforts to gain market share and increase its profits. This led one member of Binance's so-called compliance department to write, "[W]e need a banner '[I]s washing drug money too hard these days[?] [C]ome to binance[,] we got cake for you.'" This compliance employee's statement was essentially an admission that a natural and foreseeable consequence of Binance's flagrant violation of 18 U.S.C. § 1960(a) and the concomitant requirement to comply with the Bank Secrecy Act's anti-money laundering provisions was that Binance was inviting criminals to use the exchange as a laundering facility and cash-out point for its illicit cryptocurrency proceeds.

66. Brian Shroder became the CEO of Binance.US in August 2021, shortly after the Cambodian syndicate's fraud scheme against Lenny occurred. Although Zhao in fact controlled and directed BAM's and Binance.US's conduct, including BAM's efforts to mislead United States regulators and law enforcement regarding Binance's clandestine exploitation of the United States trading market in violation of 18 U.S.C. § 1960(a), Shroder agreed with Zhao that BAM should participate in and conspire with Binance's and Zhao's criminal scheme. Shroder's brother Matt worked for Binance as the head of Binance's Global Expansion Operations team. Shroder was aware, at the time that he became the Binance.US CEO, that Binance was continuing to operate in the United States market illegally, in violation of 18 U.S.C. § 1960. Shroder, however, agreed

with Zhao that BAM would maintain the public-facing position that all U.S.-based customers were restricted to using the Binance.US exchange, which had registered with FinCEN and was endeavoring to comply with United States anti-money laundering laws. Shroder knew that this public-facing position was false. Shroder also continued to publicly tout that Binance.US was "regulatorily compliant," despite knowing that Binance.US in fact was intended by Zhao to be a smokescreen to distract United States regulatory agencies and law enforcement from the fact that Binance itself was still substantially operating in the United States market and dependent on U.S.-based market makers for daily trading liquidity without registering with FinCEN or complying with the Bank Secrecy Act's anti-money laundering requirements, in violation of 18 U.S.C. § 1960(a) and the Bank Secrecy Act.

67. Incredibly, Binance and Zhao lied to and manipulated their own outside counsel, including partners at some of America's most prestigious law firms, regarding Binance's operations in the United States. This caused Binance's outside counsel, including highly respected practitioners, to unwittingly misrepresent to Article III judges that Binance was a completely foreign exchange with no U.S. operations whatsoever. Binance and Zhao used these judicial misrepresentations to evade the jurisdiction of United States courts. For example, in a civil complaint filed in the United States District Court for the Southern District of Florida pursuant to the diversity jurisdiction statute, Binance and Zhao caused its outside counsel, including a former federal prosecutor and a seasoned Supreme Court practitioner, to misrepresent to the district court in a motion to dismiss for lack of personal jurisdiction that "Binance.com . . . is not a cryptocurrency exchange for United States users—indeed, United States users are restricted from use of Binance.com." The factual admissions in Binance's and Zhao's criminal pleas have revealed and completely unraveled this lie, and so the jig is now up. As the Second Circuit Court

of Appeals found just last month, Binance in fact "has a substantial presence" in the United States, "with servers, employees, and customers throughout the country." And as the United States put it in the sentencing memorandum it filed on April 23, 2024 in Zhao's criminal prosecution, Zhao and Binance "violated U.S. law on an unprecedented scale" and "massively profited from the U.S. financial system, U.S. businesses, and U.S. customers—all without playing by U.S. rules" and "with deliberate disregard for the company's legal responsibilities and for its capacity to cause significant harm . . . ."

68. In its November 2023 criminal plea, Binance admitted that its conduct as set forth above constituted a conspiracy to violate the Bank Secrecy Act's anti-money laundering requirements and 18 U.S.C. § 1960(a)'s prohibition on operating an unregistered money transmitting business. Binance's plea to violating 18 U.S.C. § 1960(a) is necessarily an admission that every financial transaction that it conducted on the Binance exchange (*i.e.*, all of the financial transactions that occurred on the Binance exchange) were violations of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1).

69. The Commodity Futures Trading Commission ("CFTC") has also filed a complaint against Zhao and Binance in the Northern District of Illinois. *See* Dkt. 23-CV-01887. In the complaint, the CFTC alleged as follows as relevant here, making it clear that Binance's business model was predicated on money laundering and targeting U.S.-based customers to use the exchange:

a. Binance, under Zhao's direction, operating an exchange for trading commodities such as Bitcoin and Ethereum for persons in the United States since at least 2019. Dkt. 1 ¶2. 20-30% of Binance's traffic "comes from the US." ¶107.

b. Binance strategically targeting United States customers despite publicly pledging to block such customers. ¶3. Binance and Zhao also knew that doing so subjected them to U.S. law and regulations. *Id*.

c. Binance and Zhao facilitated violation of U.S. law by instructing customers in the United States to use virtual private networks to obscure their locations, allowed customers who had not submitted proof of identity to use their platform, and directed U.S. businesses and customers to incorporate shell companies to evade Binance's own compliance controls. ¶7.

d. Despite restricting access to its platform from certain jurisdictions beginning in mid-2019, Binance left open a "loophole" for customers to "sign up, deposit assets, trade, and make withdrawals without submitting to any KYC procedures as long as the customer withdrew the value of two BTC (Bitcoin) in one day. Two Bitcoin are currently worth approximately $120,000. ¶92. It was Zhao personally who implemented this policy. *Id*.

e. Zhao personally demanded that Binance *not* implement KYC on Binance.com. ¶100. And Zhao believed that if Binance's compliance controls were "too stringent" no one would use the exchange. *Id*.

f. Binance knowingly financed transactions from Hamas and senior Binance officials acknowledged with respect to other known criminals: "Like come on. They are here for crime" …. "we see the bad, but we close 2 eyes." ¶104. Binance intentionally tolerated customers using the Binance platform for illegal activity. ¶105.

g. Senior Binance officials even instructed "very closely associated with illicit activity" to open a new Binance account in order to "continue trading on the platform," which was "consistent with Zhao's business strategy." ¶106.

B. Plaintiff Lenny Licht and His Co-Plaintiffs Collectively Lost Millions of Dollars to "Pig Butchering" Schemes That Utilized the Binance Exchange and Were Facilitated by Binance's, BAM's, and Zhao's Knowing and Willful Violations of United States Law

70. A pig butchering scheme is a type of investment fraud that lures individuals into investing their money into a seemingly legitimate and profitable venture. The scheme often begins with an out-of-the-blue contact from a stranger via a social network platform, such as Facebook Messenger or WhatsApp. Using fake or stolen images, as well as personal information scraped from the internet, the stranger convinces the victim that they have common friends or business contacts. After earning the victim's trust, the stranger convinces the victim to invest money into a supposedly safe but lucrative investment opportunity. After the victim invests an initial sum of money, the stranger creates false information showing that the investment is doing well, thereby convincing the victim to invest even more money. Eventually, the stranger disappears, and the victim learns that he "invested" in a fraud scheme and that his money has been stolen.

71. Pig butchering schemes involving cryptocurrency have become increasingly common over the past decade. Criminal syndicates involved in pig butchering schemes prefer cryptocurrency because of the speed and anonymity of cryptocurrency transactions, as well as the ability to engage in transactions outside of the traditional (and highly regulated) banking system. Instead of convincing a victim to invest fiat currency into the supposed "investment," a criminal syndicate will convince the victim to purchase cryptocurrency on a well-known cryptocurrency exchange and then to transfer that cryptocurrency to the "investment" entity.

72. Because cryptocurrencies are built on public blockchains, however, cryptocurrency transactions can be tracked and traced using computer forensic analysis. This means that, unless a criminal syndicate can launder the cryptocurrency that it has stolen from the scheme's victims and convert it to fiat currency, law enforcement will, as a general matter, always be able to locate and seize the stolen assets from the criminals and return the assets to their rightful owners. Put another way, a victim of a pig butchering scheme suffers an incurable financial injury when the fraudsters successfully launder their stolen funds on an exchange such as Binance.

73. Criminal syndicates' ability to rapidly convert stolen cryptocurrency into untraceable fiat currency depends upon their ability to utilize cryptocurrency exchanges with substantial liquidity. If a criminal syndicate is unable to utilize such exchanges, it is difficult if not impossible for the syndicate to cash out of their schemes—instead, the cryptocurrency assets they stole from innocent victims will eventually be tracked, traced, and seized by law enforcement. In addition, if a cryptocurrency exchange flags a criminal syndicate's transactions as suspicious, freezes the syndicate's account, and reports the syndicate's transactions to FinCEN—as would be required by the Bank Secrecy Act—the syndicate will be prevented from cashing out of their schemes, and law enforcement can more rapidly seize the stolen assets and return them to the victims. Conversely, if a cryptocurrency exchange with substantial liquidity knowingly and willfully fails to comply with the Bank Secrecy Act and instead allows criminal syndicates to use the exchange as a laundering facility and cash-out point—which is what Binance and Zhao, with the assistance of BAM, have admitted to doing—criminal syndicates can easily cash out of the pig butchering scheme, leaving the victims completely unable to recover their stolen assets.

74. The pattern of inflows to fraudsters' Binance accounts, coupled with the accounts' cash-out activities, were themselves tell-tale signs that those Binance accounts were being used to

launder and cash out of illicit cryptocurrency assets. Accordingly, the pig butchering syndicates' use of the Binance exchange raised numerous red flags that any licensed money transmitting business making any serious effort to comply with United States anti-money laundering laws—as Binance would have been doing, but for its willful decision to flout FinCEN registration requirements, in violation of 18 U.S.C. § 1960(a)—easily would have caught and responded to, including freezing the accounts, not allowing the assets or funds in those accounts to be cashed out or withdrawn, and timely alerting FinCEN so that United States law enforcement could seize the accounts' assets before it was too late. Indeed, even if Binance had done nothing more than comply with the Bank Secrecy Act's suspicious activity reporting requirement—which, again, Binance would have done had it been operating in compliance with 18 U.S.C. § 1960(a), rather than in flagrant violation of that statute—FinCEN would have been alerted to the criminal syndicates' money laundering via the Binance exchange sufficiently early that they would not have been successful in using Binance as a cash-out point for the more than $2.7 million of USDT that was stolen from Lenny, the millions of dollars stolen from Lenny's co-Plaintiffs, and the millions more that undoubtedly was stolen by innocent victims who are not parties to this lawsuit. Binance, however, was flagrantly violating United States law, and it did so knowing that a direct, natural, and foreseeable consequence of its violations was to enable and facilitate the use of the Binance exchange as a laundering facility and cash-out point for illicit proceeds of crimes, including pig butchering schemes. Binance earned significant transaction fees on the laundering transactions.

75. If Binance had registered itself with FinCEN as a money transmitting business, rather than illegally operate as an unregistered money transmitting business in violation of 18 U.S.C. § 1960(a), Binance would have been required to comply, and would have complied, with the Bank Secrecy Act's anti-money laundering provisions. And had Binance complied with the

Bank Secrecy Act's anti-money laundering requirements, the Cambodian syndicate that defrauded Lenny of more than $2.7 million would not have been able to use Binance as a laundering facility and cash-out point, nor would the criminals who defrauded Lenny's co-Plaintiffs have been able to cash out of their pig butchering schemes. Instead, the fraudsters' efforts to launder their unlawful proceeds through Binance would have failed, their attempted laundering transactions would have been flagged as suspicious, their Binance wallets would have been frozen, law enforcement would have been able to seize the stolen assets contained in those Binance wallets, and Lenny and his co-Plaintiffs would have been able to recover all or substantially of the assets that the criminals stole from them.

76. Notably, in the few months immediately leading up to its November 2023 criminal plea, Binance started publicly touting its newfound dedication to legal compliance, including its work with law enforcement to crack down on pig butchering schemes and to help victims recover cryptocurrency assets that had been stolen from them. On August 23, 2023, for example, Binance issued a press release on its website entitled, "Binance Reports a 100% Rise in Pig Butchering Scams and Shares Tip to Prevent Them." In the press release, Binance touted its ability to use blockchain forensics to "identify and fight illicit actors in the crypto ecosystem," to "prevent criminals from benefitting from their ill-gotten gains," and to take "swift action by identifying and restricting the flow of illicit funds through the [Binance] platform." Binance stated that its "proactive investigation and monitoring work" enabled law enforcement to "recover funds" for victims of pig butchering schemes that attempted to utilize the Binance exchange as a laundering facility and cash-out point. This essentially amounts to an admission by Binance that registering with FinCEN and complying with United States anti-money laundering laws equips Binance to do the very thing that would have enabled Lenny to recover the USDT that was stolen from him—

identify suspicious transactions and users, freeze the accounts at issue, and facilitate law enforcement's seizure of the assets in the accounts and the return of those assets to their rightful owners. Indeed, Binance's Chief Communications Officer Brian Hillmann publicly stated in the summer of 2022 that "what's important to note is not where the funds come from—as crypto deposits cannot be blocked—but what we do after the funds are deposited," which would include ensuring that "any illegal funds are tracked, frozen, recovered and/or returned to their rightful owner."

77. Notably, in the 15 months since Binance began complying in earnest with the Bank Secrecy Act's anti-money laundering requirements, United States law enforcement authorities have seen a dramatic increase in the success of their efforts to recover cryptocurrency assets stolen from innocent victims by international fraud syndicates. In April 2023, for example, the United States Department of Justice announced that it had seized $112 million in cryptocurrency that one or more criminal syndicates had stolen from victims using pig butchering schemes. Using cryptography and forensic analysis, the Department of Justice and its forensic experts were able to unwind a huge, commingled network of transactions and follow the proceeds of the frauds to cash-out points at cryptocurrency exchanges, enabling the government to seize the proceeds before the criminals were able to cash out. This demonstrates that Binance's flagrant violation of FinCEN registration requirements and United States anti-money laundering laws between 2017 and October 2022 had real-world consequences for everyday people like Plaintiffs, who had fallen prey to pig butchering schemes committed by international crime syndicates.

78. Unfortunately for the Plaintiffs, during the time period that their syndicates was utilizing the Binance exchange as a laundering facility for the USDT that it stole from them, Binance was still flagrantly violating 18 U.S.C. § 1960 and the Bank Secrecy Act, including Bank

Secrecy Act's anti-money laundering requirements, and continuing to ensure that its exchange was as hospitable as possible to criminals whose illicit transactions were increasing Binance's profits. Binance also routinely ignored or failed to respond to victims' proactive requests to freeze Binance accounts that forensic analyses showed were associated with the fraud schemes that stole the victims' cryptocurrency assets.

a. Plaintiff Lenny Licht

79. In June 2021, Plaintiff Lenny Licht ("Lenny") received a Facebook friend request from a supposed woman named Tina Ling. According to her Facebook profile, "Tina Ling" was Facebook friends with one of Lenny's high school classmates. This apparent common connection convinced Lenny to accept Tina Ling's friend request, and Tina soon thereafter began communicating with Lenny via Facebook Messenger and WhatsApp. At first, it was just friendly banter. Within about a month, however, Tina Ling turned the conversation to cryptocurrency investing. Lenny had no experience with cryptocurrency, but Tina Ling convinced Lenny that he should invest his money in a supposedly successful crypto mining operation called LuxKey, which would provide both safety and positive returns.

80. Lenny, a 75-year-old widower who had lost his wife to pancreatic cancer only a few years before, fell for "Tina Ling's" false representations. Over several months, at the instruction of "Tina Ling," Lenny purchased over $2.7 million in cryptocurrency—specifically USDT (commonly referred to as "Tether"), a so-called "stable coin" that as a general matter trades at a constant market price of $1 per coin—on the regulated cryptocurrency exchanges Coinbase.com and Crypto.com. This represented almost the entirety of Lenny's life savings. Also at "Tina Ling's" instruction, Lenny transferred all of this USDT to a pair of digital wallets that he

understood to be LuxKey. The transfers were done in approximately a dozen installment transactions that occurred over a period of months.

81. LuxKey, of course, was not a cryptocurrency mining operation. It was not an investment at all. Indeed, "LuxKey" did not exist. The digital wallets to which Lenny transferred his cryptocurrency were simply self-custodied digital wallets controlled by the criminal syndicate for which "Tina Ling" was simply a fictitious front. In short, it was a scam.

82. Between approximately August 2021 and June 2022, an individual representing himself as a LuxKey customer support specialist sent repeated messages to Lenny via WhatsApp regarding the status of Lenny's "LuxKey investment." The supposed LuxKey customer support specialist also sent group messages, via WhatsApp, to Lenny and the person representing herself as "Tina Ling" regarding Lenny's "investment." These communications included numerous false statements regarding the returns that Lenny had earned on the investment and the need for Lenny to make additional payments to LuxKey to keep his investment from becoming inactive.

83. In July 2022, "Tina Ling" and "LuxKey" suddenly disappeared. Finally realizing that he had been defrauded of almost his entire life savings, Lenny contacted law enforcement and retained a private blockchain investigative agency called CipherBlade to track, trace, and recover the stolen cryptocurrency. According to CipherBlade's website, it has worked with law enforcement to recover millions of dollars in stolen cryptocurrency.

84. USDT is built on the Ethereum blockchain. Using a software program called Chainanalysis Reactor, which is used by law enforcement agencies including the FBI and the Secret Service, CipherBlade's forensic experts were able to track and trace the cryptocurrency that Lenny had sent to "LuxKey." Those wallets then transferred Lenny's USDT to "intermediary wallets" that the criminal syndicate controlled, and those intermediary wallets then transferred the

USDT to nine Binance accounts. Unfortunately, CipherBlade concluded that the Cambodian syndicate was successful in using Binance as a cash-out point, meaning that Binance allowed the syndicate to launder the USDT that it stole from Lenny and convert it into fiat currency that is untraceable and unrecoverable.

85. Each of the nine Binance accounts to which the Cambodian syndicate transferred the stolen USDT is associated with a unique identification address comprising more than 40 characters. The Cambodian syndicate's laundering of illicit funds through these nine Binance wallets began no later than August 2021. CipherBlade's analysis concluded that between August 2021 and November 2022, these nine Binance accounts received *over $40 million* of USDT across approximately 140 transactions, traceable to the two "LuxKey" wallets to which Lenny had transferred his USDT. The vast majority of the transfers (more than $34 million worth of USDT) occurred between August 2021 and July 2022. All of these money laundering transfers, including the addresses associated with the nine Binance accounts, are identified in Exhibit A appended to this complaint. CipherBlade's findings indicate that the LuxKey fraud was extensive, prolonged, and involved victims other than Lenny.

86. The nine Binance accounts to which the Cambodian syndicate transferred Lenny's USDT are no longer active, and further investigation confirmed that the wallets are essentially empty, which means the Cambodian syndicate was able to successfully use those Binance wallets as cash-out points, converting the USDT to fiat currency and leaving Lenny without any means of recovering the specific USDT assets that were stolen from him.

b. Plaintiff Zhengjun Cai

87. On or about November 28, 2021, Plaintiff Zhengjun Cai ("Cai") met a man on WeChat, a social messaging application. The man told Cai about his alleged investment in a pool that had earned him significant returns on his crypto funds. He encouraged Cai to participate.

88. On or about December 2, 2021, Cai agreed to join the pool and invest crypto funds from her self-custodial wallet. Unbeknownst to her, when she paid the nominal fee that she believed was a prerequisite to participate in pool, she was actually executing malicious code on her digital wallet that gave the scammer unfettered access to all the funds in her wallet.

89. Between December 2, 2021 and February 14, 2022, Cai made seven deposits of USDT into her digital wallet. After Cai made her initial deposit of USDT into her digital wallet, it appeared that her assets were secure and that she was earning profits on her investment.

90. However, three unauthorized withdrawals of cryptocurrency were made from Cai's digital wallet on February 3, February 7, and February 14, 2022. These fraudulent withdrawals were made without her knowledge or consent.

91. Cai's losses incurred as a result of the pig butchering scheme total $741,170.21 USDT. Cai's stolen assets comprised her life savings and funds she had set aside to refinance her home in hopes of a better life after retirement.

92. Through investigation on the public blockchain website etherscan.io, Cai has been able to verify that a substantial portion of her stolen assets were laundered through the Binance exchange.

c. Plaintiff Daniel Chang

93. On or about December 14, 2021, Daniel Chang ("Chang") was contacted by a woman on WeChat. Chang and this woman began chatting and became very friendly. The woman then introduced Chang to an investment opportunity that she claimed would pay "high interest."

94. Chang was interested in the opportunity but sought additional information about how the investment worked. The woman explained the process and convinced Chang to join and deposit USDT into his digital wallet.

95. On December 14, 2021, Chang unknowingly executed a malicious code on his wallet which enabled defrauders to access the entire wallet and make withdrawals without his consent. This code was likely disguised as an entry fee that Chang had to pay in order to participate in the investment.

96. On or about December 14, 2021, Chang began making deposits of small amounts of USDT into the investment. Over the next several weeks, Chang made four deposits of USDT into his digital wallet in order to fund the investment.

97. Initially, the investment operated in accordance with the woman's description and Chang believed he would be able to make a return on his investment. Based on this observation, Chang continued depositing USDT into his digital wallet and making larger deposits over time.

98. Between January 16, 2022 and March 11, 2022, however, Chang had a total of $289,916 USDT stolen from his digital wallet in a series of unauthorized withdrawals. The withdrawals were done without his knowledge or consent.

99. Through investigation on the public blockchain website etherscan.io, Chang has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

d. Plaintiff Henry Chen

100. On or about January 17, 2022, a person going by the name Jenny, who allegedly lived in Richmond, CA, contacted Plaintiff Henry Chen ("Chen") on Hinge. After befriending Chen, Jenny informed Chen that she was earning significant income investing cryptocurrency.

101. Having lured Chen in with the prospect of similar income, Jenny directed Chen to download an application for a digital wallet and open the link for the investment platform using the application's browser. Chen did as he was instructed.

102. Once on the investment platform's website, Jenny directed Chen to make a purchase that would allow him to participate in the investment. Chen did as he was instructed, and this action most likely executed malicious code on his digital wallet, granting scammers working with Jennie direct access to all the USDT in his digital wallet.

103. Chen deposited a total of $121,516 USDT into his digital wallet as part of the investment.

104. Between January 2022 and March 2022, scammers withdrew all the USDT from Chen's digital wallet. The withdrawals were done without Chen's knowledge or consent.

105. Through investigation on the public blockchain website etherscan.io, Mr. Chang has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

e. Plaintiff Dominic Chow

106. On or about January 19, 2022, Plaintiff Dominic Chow ("Chow") met an individual named Eileen Chou on WhatsApp. Chou told Chow about an investment opportunity for cryptocurrency using a particular digital wallet.

107. After about 2 months, Chow decided to participate in the investment. Eileen directed Chow to purchase a voucher using his digital wallet in order to participate in the investment, which Chow did on March 8, 2022.

108. Unbeknownst to Chow, he was actually executing a malicious code on his wallet that gave scammers working with Eileen perpetual and unlimited access to withdraw all the USDT in his account.

109. Between March 8, 2022 and March 18, 2022, Chow deposited a total of $280,914 USDT into his digital wallet to participate in the liquidity mining pool.

110. Scammers withdrew all these funds from his digital wallet without his knowledge or consent.

111. Through investigation on the public blockchain website etherscan.io, Chow was able to verify that a substantial portion of his stolen assets has been laundered through the Binance exchange.

112. Chow promptly reached out to Binance for assistance in freezing the wallets and recovering his funds. Binance responded that the wallet(s) belonged to "SafePal," a "Binance Broker," with many users whose identities are unknown to it.

113. Binance told Chow that Binance "was not responsible for the management of the assets on the broker's wallet so [it was] unable to help [Chow] track the funds further."

f. Plaintiff Chengguo Dong

114. On or about October 26, 2021, Plaintiff Chengguo Dong ("Dong") was approached by an individual on Line, a social media application.

115. The individual extended Dong an investigation to participate in an investment opportunity using funds from his digital wallet.

116. On or about October 27, 2021, Dong purchased a voucher using funds in his digital wallet in order to start investing. Dong had no idea that, by purchasing the voucher, he had executed malicious code on his wallet that allowed third parties to withdraw all the USDT in his digital wallet.

117. Between October 29, 2021 and November 12, 2021, Dong made several deposits of USDT into his digital wallet in order to participate in the investment. These funds comprised his life savings.

118. On November 12, 2021, fraudsters drained Dong's entire digital wallet, leaving him with nothing. Dong, a 50-year-old Chinese immigrant residing in Burlingame, California, had been planning to use the funds to purchase a home for his family, as well as pay his daughter's educational expenses.

119. Through investigation on the public blockchain website etherscan.io, Dong has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

g. Plaintiff Amine Fennane

120. On March 15, 2022, a person going by the name of Angela Andrew, who allegedly lived in Paris, contacted Plaintiff Amine Fennane on Instagram. After befriending Fennane through social media, Andrew introduced him to an investment pool that Andrew insisted he join using his digital wallet.

121. Andrew told Fennane to pay a network fee in order to join the investment pool using the funds in his digital wallet, which Fennane did. This action most likely executed a malicious code on Fennane's wallet permitting third-party scammers working with Andrew to withdraw all the USDT in his digital wallet.

122. To fund the pool, Fennane deposited a total of $160,307 in USDT into his digital wallet.

123. Between April 6, 2022, and May 9, 2022, scammers withdrew all the USDT from Fennane's digital wallet without his knowledge or consent.

124. Fennane lost not only his life savings as a result of the fraud, but he also had to take out loans from his family and financial institutions.

125. Through investigation on the public blockchain website etherscan.io, Fennane has been able to verify that a substantial portion of his stolen crypto funds were laundered through the Binance exchange.

h. Plaintiff Ihab William Francis

126. On or about September 18, 2021, Plaintiff Ihab William Francis ("Francis") was contacted by an individual on LinkedIn who described himself as a cryptocurrency investor offering to explain to Francis how he had successfully made money in the cryptocurrency market. The individual offered Francis a "time-limited opportunity" to earn interest in an investment pool using cryptocurrency in a digital wallet.

127. As part of the fraudulent pool scheme, Francis was directed to "join the node" and receive a voucher into his digital wallet in order to join the pool. Francis did as he was instructed, and in the process unknowingly executed malicious code that permitted third-party scammers to withdraw all the USDT in his digital wallet.

128. After joining the pool through, Francis made small transfers to the pool from his digital wallet on November 3 and 8, 2021. The initial contributions appeared to be yielding interest in accordance with Francis's understanding, so he continued to make contributions.

129. Francis made 12 deposits of USDT into his digital wallet between November 3, 2021 and January 10, 2022.

130. Francis had all the funds in his digital wallet withdrawn without his knowledge or consent in a series of four swipes. All told, Francis had $462,883.48 USDT stolen.

131. The losses incurred by Francis as a result of the scheme included assets that Francis had withdrawn from his 401K, Roth IRAs, and family's personal savings accounts. Francis was left without any savings or retirement funds, leaving him and his family in financial ruin.

132. Through investigation on the public blockchain website etherscan.io, Francis has been able to verify that a substantial portion of his stolen crypto assets were laundered through the Binance exchange.

i. Plaintiff John Gordon

133. On or about June 1, 2022, a person going by the name "Laura", who allegedly lived in New York, contacted Plaintiff John Gordon through social media. After befriending Gordon, Laura informed him about her interest in cryptocurrency and her successful investment in cryptocurrency using a digital wallet.

134. Having lured Gordon in with the prospect of similar income, Laura directed Gordon to access the investment platform using his digital wallet. Gordon did as he was instructed, not realizing that at one point he executed malicious code that gave scammers unlimited and perpetual access to the funds in his digital wallet.

135. On or about June 10, 2022, Gordon began making small deposits into his digital wallet to test the investment platform.

136. After the initial deposits earned the promised interest on his original investment, Gordon continued to make additional deposits. Between June 10 and June 23, 2022, Gordon made 8 deposits of USDT into his digital wallet.

137. All the USDT in Gordon's digital wallet was then fraudulently withdrawn in unauthorized transactions.

138. Gordon lost his life savings and other funds needed to support his dependent father.

139. Through investigation on the public blockchain website etherscan.io, Gordon has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

j. Plaintiff Shai Granovski

140. On October 20, 2021, a person going by the name Miriam, who allegedly lived in Hong Kong, contacted Plaintiff Shai Granovski through Instagram and informed him of a supposed pool in which he could invest cryptocurrency. Miriam ostensibly was an online friend (*i.e.*, Facebook friend) of one of Granovski's longtime friends. This convinced Granovski of Miriam's legitimacy.

141. After gaining Granovski's trust, Miriam directed Granovski to purchase a "node" to join the investment pool using funds in his digital wallet. Granovski did as he was instructed, and this action most likely executed malicious code that gave Miriam (who in reality were scammers acting under a fictitious name) unlimited and indefinite access to all the USDT in his digital wallet.

142. To fund the pool, Granovski deposited a total of $517,477 in USDT into his digital wallet, virtually his entire life savings.

143. On or around December 9, 2021, scammers withdrew all the USDT from Granovski's digital wallet. This withdrawal was done without Granovski's knowledge or consent.

144. Through investigation on the public blockchain website etherscan.io, Granovski has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

k. Plaintiff Dalton Green

145. On or about December 4, 2021, after hearing about an investment opportunity that was earning significant income from his friends, Plaintiff Dalton Green ("Green") decided to join, what he and his friends thought was a legitimate investment pool.

146. Green accessed the platform using his digital wallet. Green used funds from his digital wallet to purchase a voucher that would allow him to join the pool. This action most likely executed malicious code that gave third parties access to all the USDT in his wallet.

147. To fund the pool, Green deposited a total of $71,096 USDT into his digital wallet.

148. In December 2021, scammers withdrew all the USDT from his digital wallet. The withdrawal was done without Green's knowledge or consent.

149. Green's life has been devastated both financially and emotionally. The financial loss caused a great deal of stress to, and ultimately ended, his marriage, triggering a spiraling depression.

150. Through investigation on the public blockchain website etherscan.io, Green has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

l. Plaintiff Michael Grilli

151. On or around November 11, 2021, Plaintiff Michael Grilli met a woman through a social media website. After befriending Grilli, the woman encouraged him to join a cryptocurrency investment pool from which she insisted Grilli would be able to earn significant income.

152. The woman directed Grilli to deposit USDT into his digital wallet and open the link for the pool from his wallet's browser.

153. Unbeknownst to Grilli, by following the woman's instructions, he provided scammers the ability to execute malicious code on his wallet, which then allowed the scammers to withdraw all of the USDT from his digital wallet without his authorization or consent.

154. Between December 2021 to March 2022, scammers, through unauthorized transactions, stole all of the USDT Grilli deposited in his digital wallet, amounting to approximately $3,718,480.

155. The financial loss has devastated Grilli. Grilli, age 83, saw his savings depleted and had taken out multiple loans to fund his digital wallet. As a result of his grave financial loss, he has suffered significant mental and emotional distress and anxiety.

156. Through investigation on the public blockchain website etherscan.io, Grilli has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

m. Plaintiff Iraklis Karabassis

157. In or around January 2022, Plaintiff Iraklis Karabassis met a woman going by the named Zhu Bella Hannah Ziaohan Zhu ("Hannah") on Instagram.

158. Through subsequent correspondence and phone calls, Hannah presented Karabassis with the opportunity to invest in a very lucrative cryptocurrency investment pool using a digital

crypto wallet. Hannah instructed Karabassis to download the required digital wallet application and then transfer crypto into his account.

159. Under the guise of giving Karabassis access to the pool, Hannah sent him a voucher to through which he would receive a nominal amount of crypto into his digital wallet. Karabassis did as Hannah instructed and accepted the voucher, unwittingly executing malicious code on his wallet that would allow the scammers working with Hannah unfettered access to all the USDT in his digital wallet.

160. Over the next several weeks, Karabassis transferred $1,180,760 USDT into his digital wallet to participate in the pool.

161. On March 4, 2022, scammers transferred $1,180,760 USDT out of Karabassis's digital wallet without his knowledge or consent.

162. A month later, Karabassis deposited another $4,899 USDT into his digital believing that this would allow him to regain access to his $1,180,760 USDT and to the interest that it had allegedly accrued. The scammers subsequently withdrew that amount from his wallet as well.

163. Through investigation on the public blockchain website etherscan.io, Karabassis has been able to verify that a substantial portion of his stolen assets, proceeds of the crime, were laundered through the Binance exchange.

n. Plaintiff Alicia Lau

164. On or around May 29, 2021, a person going by the name of Toby, who allegedly lived in London, contacted Plaintiff Alicia Lau ("Alicia Lau") through Instagram. After befriending Alicia Lau, Toby encouraged Alicia Lau to join an investment pool from which he insisted she would be able to earn significant income investing in cryptocurrency.

165. "Toby" directed Alicia Lau to deposit USDT into her digital wallet. Toby then directed Lau to open the link for the pool in the browser of her digital wallet and provided Alicia Lau with a "voucher" to register for and to join the pool.

166. Unfortunately for Alicia Lau, she had unsuspectingly given scammers access to all the funds in her digital wallet when she joined the pool.

167. To fund the pool, Alicia Lau deposited a total of $205,744 USDT into her digital wallet.

168. Between October 7, 2021, and December 2, 2021, the scammers, through unauthorized transactions, stole all of the USDT in Alicia Lau's digital wallet. These fraudulent withdrawals were done without Alicia Lau's knowledge or consent.

169. Alicia Lau lost her life savings, has gone into substantial debt, and suffers from depression because of the scam.

170. Through investigation on the public blockchain website etherscan.io, Alicia Lau has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

o. Plaintiff Trevor Lau

171. In January 2022, a person going by the name Abby, who supposedly lived in San Francisco, contacted Plaintiff Trevor Lau ("Trevor Lau") on Twitter. (Trevor Lau is not related to Alicia Lau.) After befriending Trevor Lau, Abby informed Trevor Lau that she was earning significant income by participating in a cryptocurrency investment pool.

172. Having lured Trevor Lau in with the prospect of similar income, Abby directed Trevor Lau to download the necessary digital wallet and open the link using the wallet's browser.

Trevor Lau followed Abby's instructions. Unbeknownst to Trevor Lau, the investment pool was simply a fraud.

173. Once on the fraudulent pool's site, Abby directed Trevor Lau to purchase a node that would allow him to join the pool. Lau again did as he was instructed, unsuspectingly executing malicious code that gave scammers access to all the funds in his digital wallet.

174. To fund the pool, Lau deposited a total of $250,327 USDT into his digital wallet.

175. In January 2022, scammers withdrew all the USDT from Lau's digital wallet. The fraudulent withdrawal was done without Lau's knowledge or consent.

176. The funds stolen from Lau's digital wallet represented his life savings.

177. Through investigation on the public blockchain website etherscan.io, Lau has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

p. Plaintiff Nader Lobandi

178. On or around March of 2022, a person going by the name of Aimee contacted Plaintiff Nader Lobandi ("Lobandi") through social media. After befriending Lobandi, Aimee encouraged him to join a cryptocurrency investment pool from which she insisted he would be able to earn significant income. She directed Lobandi to deposit USDT into his digital wallet to contribute to the pool.

179. Aimee then directed Lobandi to open a link that she provided him in his digital wallet browser. Aimee directed him to click a button to "join the node" and start participating in the pool. Unbeknownst to Lobandi, this action allowed scammers to access and initiate transfers from his digital wallet without his knowledge or consent.

180. On or around April 12, 2022, scammers, through unauthorized transactions, stole all of the USDT from Lobandi's digital wallet, amounting to approximately $92,640 USDT. These withdrawals were done without Lobandi's knowledge or consent.

181. Lobandi lost a significant portion of his life savings and suffered emotional and mental distress as a result of these unauthorized transactions. Due to the mental distress Lobandi experienced soon after the incident, he was hospitalized for two weeks for severe anxiety and depression.

182. Through investigation on the public blockchain website etherscan.io, Lobandi has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

q. Plaintiff Eisi Mollanji

183. On or about March 28, 2022, a person going by the name Aiden, who supposedly lived in Ottawa, contacted Plaintiff Eisi Mollanji ("Mollanji") on the dating app Hinge. At the time, Mollanji was a medical school student preparing for his residency.

184. After befriending Mollanji, Aiden informed Mollanji about an opportunity to make huge profits through targeted swing trades on a platform called "Coincheck." At Aiden's insistence, Mollanji joined Coincheck and deposited $60,000 USDT into Coincheck.

185. Once Mollanji's account reached $120,000 USDT, Coincheck's "customer service" contacted Mollanji and notified him that if he wanted to withdraw his funds, he would need to comply with Coincheck's money laundering regulations and show proof that he already held $100,000 USDT. Aiden assured Mollanji that the same verification was required for all users.

186. Coincheck's "customer service" informed Mollanji that he would need to verify the proof of funds by demonstrating he had the funds available in a particular digital wallet. Mollanji

was desperate to get his money back, so he downloaded the supposedly necessary digital wallet application, obtained a wallet, and deposited $100,471 USDT into it.

187. On or about April 20, 2022, scammers withdrew all of the USDT from Mollanji's digital wallet. This withdrawal was done without Mollanji's knowledge or consent.

188. Mollanji's life has been devastated by the scheme. Mollanji borrowed the money to fund his digital wallet on a professional student line of credit, and the theft essentially left Mollanji impoverished.

189. Through investigation on the public blockchain website etherscan.io, Mollanji has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

r. Plaintiff James Moskwa

190. On or around October 10, 2021, Plaintiff James Moskwa ("Moskwa") was introduced to a woman named "Tresa" on Instagram.

191. Over several weeks, Moskwa began to develop a friendship with Tresa. Moskwa and Tresa spoke often, and she eventually brought up the topic of crypto investments. Tresa told Moskwa that her uncle was assisting her in making investments. She told Moskwa that her uncle was a broker involved in a cryptocurrency investment opportunity. Tresa convinced Moskwa to obtain the required digital wallet and participate in the investment pool as well. She eventually introduced Moskwa to her uncle to have him describe the technicalities of the pool.

192. On or around November 1, 2021, Moskwa obtained his digital wallet, and Tresa walked Moskwa through the process of purchasing the needed entry voucher on the wallet application. Moskwa purchased the voucher using cryptocurrency that Tresa sent him.

193. Unbeknownst to him, by accepting cryptocurrency from Tresa, Moskwa actually had executed malicious code on his wallet, allowing scammers working with Tresa access to all the USDT in his wallet.

194. On or about November 16, 2021, Moskwa started depositing USDT into his digital wallet. Between November 16, 2021 and January 21, 2022, Moskwa made six deposits into his digital wallet to participate in the pool.

195. Between December 24, 2021 through January 21, 2022, scammers withdrew all the USDT from Moskwa's digital wallet.

196. Shortly after the unauthorized withdrawals, Moskwa contacted the pool's supposed customer service department to inform the pool of the fraudulent withdrawals. The customer service agent informed Moskwa that his account was temporarily frozen and that he would have to deposit an additional $262,798.00 for "account risk verification" to unfreeze his account and access his assets.

197. Fearful of losing the hundreds of thousands of dollars he already had deposited, Moskwa agreed to comply with the request and continued to make additional deposits of USDT. These funds were also withdrawn from his digital wallet without his knowledge or consent.

198. All told, Moskwa lost $1,417,654.06 USD because of the fraudulent withdrawals. These funds comprised his life savings, retirement fund, and even some personal loans from friends. As a result of the scam, Moskwa had to refinance his mortgage and incurred substantial tax penalties from premature withdrawals from his retirement accounts. The substantial financial loss has caused him significant emotional distress.

199. Through investigation on the public blockchain website etherscan.io, Moskwa has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

s. Plaintiff Anh Nguyen

200. On or about October 16, 2021, Plaintiff Anh Nguyen ("Nguyen") was contacted by a woman named "Teyana Cuffe" on Facebook. After befriending Nguyen, this individual informed him of a cryptocurrency investment opportunity using a digital wallet.

201. Having convinced Nguyen that he could gain significant returns on USDT investments through the investment pool, Teyana directed Nguyen to open a link to the platform he was sent and purchase a voucher to start investing. Nguyen was instructed that he had to deposit USDT into his digital wallet to collect interest through the pool.

202. On or about October 29, 2021, Nguyen did as he was instructed and purchased a voucher. Unbeknownst to Nguyen, he had executed malicious code that allowed scammers direct, unlimited, and indefinite access to funds in his digital wallet.

203. Initially, the pool operated as described and Nguyen appeared to earn interest on his deposited USDT.

204. However, on or about October 29, 2021, all the USDT was removed from Nguyen's digital wallet by scammers. When Nguyen inquired to the pool's supposed customer service department about the withdrawal, he was told that his assets had been contributed to a "special pool" in order to yield higher earnings and that all of his funds were still in his digital wallet.

205. Nguyen was also informed that he needed to contribute another $200,000 USDT into his digital wallet in order to regain access to his assets and earn his reward. On or about

November 18, 2021, Nguyen deposited additional USDT into his wallet to meet the $200,000 USDT threshold requirement.

206. Immediately after his wallet reached $200,000 USDT, the scammers drained his digital wallet again. All told, Nguyen lost a total of $222,946 USDT because of the fraudulent transactions.

207. The financial and emotional results of the loss have been devastating for Nguyen and his family, causing significant mental anguish and suicidal thoughts. Nguyen and his wife have lost the majority of their life savings and are struggling to make ends meet.

208. Through investigation on the public blockchain website etherscan.io, Nguyen has been able to verify that a significant portion of his stolen assets were laundered through the Binance exchange.

t. Plaintiff Brian Rothaus

209. On or around April 11, 2022, a woman contacted Plaintiff Brian Rothaus ("Rothaus") through Facebook under the guise of seeking golf advice from Rothaus, who is an avid golfer. After chatting with Rothaus about golf, the woman told Rothaus about her investments in cryptocurrency and asked Rothaus to participate in an investment pool. The woman directed Rothaus to obtain the necessary digital wallet and to deposit USDT into the wallet. The woman told Rothaus that he could easily transfer the funds from his digital wallet to his personal account.

210. The woman then directed Rothaus to open the link for the pool in his digital wallet browser.

211. Rothaus made one deposit of 247,456.34 USDT into his digital wallet on or around October 26, 2022. On or around October 27, 2022, Rothaus clicked a button to "receive" a node

and participate in the pool, which unknowingly executed malicious code on his digital wallet giving scammers direct and unlimited access to his account.

212. Later that same day, scammers stole all of the USDT in Rothaus's digital wallet totaling approximately $247,456 USDT. This withdrawal was done without his knowledge or consent.

213. Rothaus lost his IRA savings as a result of this scam and suffered substantial emotional and mental distress due to the financial loss.

214. Through investigation on the public blockchain website etherscan.io, Rothaus has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

u. Plaintiff Gordon Shaylor

215. On or around December 17, 2021, Plaintiff Gordan Shaylor ("Shaylor") was contacted by a woman named Sa Li through Facebook. After befriending Shaylor, Sa Li began communicating with him on WhatsApp and encouraged Shaylor to join a cryptocurrency investment pool, which she assured Shaylor was a safe investment opportunity.

216. To join the pool, Sa Li directed Shaylor to obtain a digital wallet using a specific application and deposit USDT into the wallet.

217. Shaylor was then instructed to open the link for the pool through the wallet application's browser. Shaylor was instructed to purchase a "node," which unbeknownst to him executed malicious code on his digital wallet and provided scammers unfettered access to the wallet.

218. To fund the supposed pool, Shaylor made multiple deposits of USDT into his digital wallet over the course of nine months. The pool then fraudulently reported to Shaylor that he was

earning significant interest on his deposits, which convinced Shaylor to heed Sa Li's advice to continue to deposit more and more money into his digital wallet. In truth, Sa Li was simply a fictious name under which scammers were operating.

219. On or around August 2022, the scammers stole all of the USDT in Shaylor's digital wallet, amounting to approximately $1,200,000. The fraudulent withdrawal was done without Shaylor's permission or consent.

220. As a result of the fraud scam, Shaylor lost all of his life savings at age 60 and has incurred substantial debt from loans taken during the process. He also experienced significant anxiety and emotional distress due to the financial loss.

221. Shaylor subsequently retained the services of forensic crypto tracers who concluded with "very strong confidence" that the scammers utilized the Binance exchange to launder the assets they stole from Shaylor.

v. Plaintiff Richard Slavant

222. On or about September 27, 2021, a woman contacted Plaintiff Richard Slavant ("Slavant") on WhatsApp. After befriending Slavant, the woman informed him that she was earning significant income on her cryptocurrency by participating in an investment pool.

223. Having lured Slavant in with the prospect of similar income, the woman directed Slavant to download an application and obtain a digital wallet. She then instructed him to open a link using the digital wallet application's browser. Slavant complied, not realizing that the supposed investment pool was simply a fraud.

224. Once on the fraudulent pool's site, the woman directed Slavant to purchase a node that would allow him to join the pool. On or about October 8, 2021, Slavant did as he was

instructed and unknowingly executed malicious code that gave scammers direct and unfettered access to all the USDT in his digital wallet.

225. Between October 9 and November 9, 2021, Slavant made four deposits of USDT into his digital wallet to fund the pool.

226. On or about November 13, 2021, scammers withdrew all the USDT from Slavant's digital wallet. The fraudulent withdrawal was done without Slavant's knowledge or consent.

227. As a result of the scam, Slavant lost approximately $52,349.87 USDT, comprised of funds from loans and other personal savings. The scam has been devastating to Slavant, both financially and emotionally, and resulted in significant distress.

228. Through investigation on the public blockchain website etherscan.io, Rothaus been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchage.

w. Plaintiff Nathanial Thrailkill

229. On or about December 4, 2021, after hearing about an investment opportunity that was earning significant income from his friends, Plaintiff Nathanial Thrailkill ("Thrailkill") decided to join what they all thought was a cryptocurrency investment pool.

230. Thrailkill accessed the platform for the supposed pool using the application for his digital wallet on both his phone and desktop.

231. Between December 7, 2021 and December 8, 2021, Thrailkill made 3 deposits totaling approximately $100,308 USDT to fund the pool.

232. Once Thrailkill's money was deposited into his wallet, he was told to accept a voucher in order to pay the "mining fee" so that he could begin "investing." Unbeknownst to

Thrailkill, by accepting the voucher, he executed malicious code that allowed scammers to gain access to and withdraw his USDT.

233. On December 10, 2021, mere hours after making his last deposit, scammers stole all the USDT in Thrailkill's digital wallet. The fraudulent withdrawal was done without Thrailkill's knowledge or consent.

234. Thrailkill lost his entire life savings, resulting in significant emotional and mental distress.

235. Through investigation on the public blockchain website etherscan.io, Thraikill has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

x. Plaintiff Jack Yao

236. On or around May 30, 2022, Plaintiff Jack Yao ("Yao") was introduced to a cryptocurrency investment pool opportunity by his friend, Plaintiff Tao Wang ("Wang"), who had been contacted by a woman named Li Zhu on WeChat.

237. After communicating with Wang about the investment pool, Yao agreed to join the pool as well. Unfortunately, both Wang and Yao were victims of a fraud.

238. On or around May 30, 2022, Yao deposited USDT into his digital wallet and opened the provided link for the pool's platform through the browser on his digital wallet application.

239. To fund the pool, Yao made 6 deposits of USDT into his digital wallet.

240. On or around June 29, 2022, scammers drained Yao's digital wallet of all the USDT that he had deposited into it. Yao promptly contacted Wang, who informed him that his wallet had also been drained. Yao immediately contacted the pool's supposed customer service department about the unauthorized withdrawal, and he was informed that his account had been "frozen" and

that his USDT had been "transferred to a custodian account because they detected abnormal activit[y]."

241. The supposed customer service representative then instructed Yao that he would have to deposit additional funds into his digital wallet in order to unfreeze his account. On or around July 7, 2022, Yao, desperate to retrieve his crypto, complied with the demand and deposited additional funds into his digital wallet. Hours later, Yao's digital wallet was drained again.

242. Scammers, through unauthorized transactions on June 29 and July 9, 2022, had stolen all of the USDT in Yao's digital wallet, totaling $310,000 USDT. These withdrawals were done without his knowledge or consent.

243. Yao has lost his entire life savings and suffered significant mental and emotional distress as a result of the unauthorized transactions.

244. Through a forensic blockchain investigation conducted by the firm CoinStructive, Yao was able to determine that a substantial portion of his stolen assets were laundered through the Binance exchange.

y. Plaintiff Edmund Yeo

245. On November 16, 2021, a person going by the name Juli Chua contacted Plaintiff Edmund Yeo through WhatsApp. After befriending Yeo, Chua introduced Yeo to an investment pool and directed Yeo to join using a digital wallet application.

246. Chua directed Yeo to visit the pool through the wallet browser. On November 23, 2021, Yeo, at the direction of Chua, registered for the pool through his digital wallet and pressed "confirm" to purchase a "voucher." This action very likely executed malicious code on his wallet that gave scammers unfettered and unlimited access to the funds therein.

247. To fund the pool, Yeo deposited a total of $346,652 USDT into his digital wallet.

248. Between December 8, 2021, and January 7, 2022, scammers withdrew all of the USDT from Yeo's digital wallet. These fraudulent withdrawals were done without Yeo's knowledge or consent.

249. Yeo lost his entire life savings and retirement fund because of these unauthorized transactions. This experience has brought a lot of financial, mental, and emotional stress into Yeo's life. In addition to losing his life savings, he lost his mother's and sister's life savings as well.

250. Through investigation on the public blockchain website etherscan.io, Yeo has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

z. Plaintiff Jun Zhai

251. On or about February 23, 2022, a person going by the name "Julie", who supposedly lived in Seattle, contacted Plaintiff Jun Zhai ("Zhai") on WeChat. Julie told Zhai that she was in the cosmetic surgery industry and was visiting San Diego, California on a business trip. After befriending Zhai, Julie told him about her hobbies and informed Zhai that she was earning significant income participating in a cryptocurrency investment pool.

252. Zhai believed the pool was legitimate and agreed to participate. Julie directed Zhai to download a digital wallet application and to open the link for the pool using the digital wallet's browser. On or about February 28, 2022, Zhai did as he was instructed and purchased a voucher to begin transferring funds into his digital wallet. In the process, he unsuspectingly executed malicious code on his wallet that gave scammers unfettered and unlimited access to the assets in his digital wallet.

253. Between March 2 and March 22, 2022, Zhai made four deposits of $69,747 USDT into his digital wallet to fund the pool.

254. On or about April 5, 2022, scammers withdrew all the USDT from Zhai's digital wallet. The withdrawal was done without Zhai's knowledge or consent.

255. Zhai lost his entire retirement fund and life savings as a result of the scam. The scam led Zhai to be depressed and negatively impacted his job performance.

256. Through investigation on the public blockchain website etherscan.io, Zhai has been able to verify that a substantial portion of his stolen assets were laundered through the Binance exchange.

V. THE DEFENDANTS' CIVIL RICO LIABILITY

A. The RICO Enterprises

257. Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 256 above.

258. Binance and BAM constituted an association-in-fact RICO enterprise, the common purpose of which was to enable Binance to operate an unlicensed, unregistered money transmitting business under the false pretenses that Binance was not available to U.S.-based customers and that U.S.-based customers would only be allowed to transact on BAM's Binance.US cryptocurrency exchange, which in turn would enable Binance to avoid complying with the Bank Secrecy Act's anti-money laundering requirements, including the obligation to conduct "Know Your Customer" diligence, monitor the Binance exchange for suspicious transactions, flag suspicious transactions, report such transactions to FinCEN, and freeze accounts associated with suspicious transactions or individuals or entities flagged during the "Know Your Customer" diligence process. This association-in-fact enterprise is referred to herein as "Enterprise #1." Binance, BAM, and Zhao participated in and conducted the affairs of Enterprise #1 through a pattern of racketeering activity.

259. Zhao and the individual Binance and BAM employees, officers, and executives with whom Zhao conspired to violate 18 U.S.C. § 1960(a)—including BAM's then-CEO Briah Shroder and the persons identified in the Binance plea agreement's Statement of Facts as Individuals 1, 2, 3, and 4, all of whom are known to Binance, BAM, and Zhao—constituted an association-in-fact enterprise, the common purposes of which was (1) to allow Binance to operate as an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960(a); (2) to allow Binance to conduct financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i); and (3) to allow Binance to operate in a manner that was hospitable to, and would facilitate, the laundering of illicit proceeds on the Binance exchange, including cryptocurrency assets that had been stolen from United States citizens through schemes to defraud, all in violation of 18 U.S.C. § 1956(a)(1)(A)-(B). This association-in-fact enterprise is referred to herein as Enterprise #2. Zhao directed the conduct of Enterprise #2's affairs through a pattern of racketeering activity.

260. Insofar as Zhao and his Binance employees, officers, and executives conspired to operate Binance, systematically and continuously for more than five years, as an inherently illegal money transmitting business in violation of 18 U.S.C. § 1960(a), with every transaction that Binance conducted on the Binance exchange also being a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1), Binance itself is a corporate RICO enterprise, the conduct for which Zhao can be held responsible as the RICO defendant. The Binance corporate RICO enterprise is referred to herein as Enterprise #3. Defendant Zhao, as then-CEO and mastermind of the Binance corporate RICO enterprise, may be held individually liable for directing that corporate RICO enterprise to operate through a pattern

of racketeering activity. In addition, Defendant BAM may be held liable for conspiring with that corporate RICO enterprise's pattern of racketeering activity.

261. Binance, Zhao, and each of the criminal syndicates that were engaged in ongoing, extensive cryptocurrency fraud schemes that victimized American citizens and utilized the Binance exchange as a laundering facility and cash-out point also constituted association-in-fact RICO enterprises, the common purpose of which was to allow the syndicate(s) to use the Binance exchange, in return for substantial transaction fees paid to Binance, as a laundering facility and a cash-out point for the syndicate(s) ongoing, extensive fraud schemes. Because it is not presently known whether the Plaintiffs were victimized by a single common syndicate or multiple syndicates (which ultimately is inconsequential to Defendants' RICO liability), the associate-in-fact comprised of Binance, Zhao, and the criminal syndicate(s) that defrauded each of the Plaintiffs is referred to herein as "Enterprise #4." Binance and Zhao participated in the conduct of Enterprise #4's affairs through a pattern of racketeering activity, because they participated in the operation of Enterprise #4's money laundering and cash-out activities that utilized the Binance exchange.

262. Each of the criminal syndicates that defrauded the Plaintiffs of millions of dollars also constituted a discrete association-in-fact enterprise, the common purpose of which was to steal cryptocurrency assets and then launder the stolen assets on cryptocurrency exchanges (including Binance) that were unregistered with FinCEN, had lax or nonexistent "Know Your Customer" and anti-money laundering policies, and had enough daily liquidity to serve as readily available cash-out points. Because it is not presently known whether the Plaintiffs were victimized by a single common syndicate or multiple syndicates (which ultimately it inconsequential to Defendants' RICO liability), these association-in-fact enterprises are referred to herein, collectively, as "Enterprise #5." Binance and Zhao conspired with Enterprise #5's pattern of racketeering activity,

namely Enterprise #5's use of the Binance exchange as a laundering facility and cash-out point for the cryptocurrency assets that Enterprise #5 fraudulently stole from the Plaintiffs and countless other victims who are not parties to this lawsuit.

B. The RICO Enterprises' Patterns of Racketeering Activity

263. Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 262 above.

264. With respect to Enterprise #1, Binance, BAM, and Zhao participated in and/or directed the enterprise's affairs through a pattern of racketeering activity, to wit, operating Binance as an unregistered and unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a) while misleading United States regulators and law enforcement into believing that all U.S.-based customers were being routed to the registered Binance.US exchange. Because the Binance exchange operated in violation of 18 U.S.C. § 1960(a), and because a violation of 18 U.S.C. § 1960(a) is a RICO predicate under 18 U.S.C. § 1961(1)(B), every financial transaction that Binance conducted on the Binance exchange was a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1). Accordingly, Enterprise #1's pattern of racketeering included serial, years-long violations of 18 U.S.C. § 1956, in addition to the serial, years-long violations of 18 U.S.C. § 1960(a). Enterprise #1 and its pattern of racketeering activity began in or around June 2019, when BAM formed Binance.US and registered it with FinCEN to divert United States regulators' and law enforcement's attention away from Binance and ran until at least October 2022. On information and belief, Enterprise #1's pattern of racketeering activity would have continued indefinitely had the United States Department of Justice not conducted its investigation and ultimately its prosecution of Binance and Zhao.

265. With respect to Enterprise #2 and Enterprise #3, Zhao was associated with and directed the conduct of each of those enterprises through a pattern of racketeering activity, to wit, operating Binance as an unregistered and unlicensed money transmitting business in violation of 18 U.S.C. § 1960(a), while misleading United States law enforcement into believing that all United States customers were being routed exclusively to the registered and licensed Binance.US exchange. Because the Binance exchange operated in violation of 18 U.S.C. § 1960(a), and because a violation of 18 U.S.C. § 1960(a) is a RICO predicate under 18 U.S.C. § 1961(1)(B), every financial transaction that Binance conducted on the Binance exchange was a violation of 18 U.S.C. § 1956(a)(1)(A)(i) by virtue of 18 U.S.C. § 1956(c)(7)(A)'s cross-reference to 18 U.S.C. § 1961(1). Accordingly, Enterprise #2's and Enterprise #3's patterns of racketeering included serial, years-long violations of 18 U.S.C. § 1956, in addition to the serial, years-long violations of 18 U.S.C. § 1960(a). Enterprise #2 and Enterprise #3, and their patterns of racketeering activity, began in or around July 2017, when Zhao launched Binance, and ran until at least October 2022. On information and belief, Enterprise #2's and Enterprise #3's pattern of racketeering activity would have continued indefinitely had the United States Department of Justice not commenced its investigation and ultimately its prosecution of Binance and its Zhao.

266. With respect to Enterprise #4, Binance and Zhao were associated with and participated in the conduct of the enterprise's affairs through a pattern of racketeering activity, to wit, knowingly allowing the pig butchering syndicates to use the Binance exchange to engage in numerous cryptocurrency transactions involving illicit proceeds, such transactions being intended to promote and facilitate the syndicate's underlying wire fraud schemes, to conceal the nature and source of the stolen cryptocurrency assets, and to enable the conversion of the stolen assets to untraceable fiat currency, in violation of 18 U.S.C. § 1956(a)(1)(A)-(B). Enterprise #4's period of

racketeering activity began no later than August 2021 and ended no earlier than November 2022. With respect to the fraud scheme against Lenny alone, each of the transactions that the Cambodian syndicate conducted using the nine Binance wallets through which it laundered and cashed out Lenny's stolen cryptocurrency constituted a violation of 18 U.S.C. § 1956(a)(1)(A)-(B), amounting to dozens of violations spanning roughly a year. On information and belief, Enterprise #4's pattern of racketeering activity would have continued indefinitely, and would have involved more victims and more money laundering on the Binance exchange, had the United States Department of Justice not commenced its investigation and ultimately its prosecution of Binance and Zhao for violations of 18 U.S.C. § 1960(a) and the Bank Secrecy Act.

267. Enterprise #5 engaged in a pattern of racketeering activity, to wit, using international wire communications to defraud Lenny and U.S.-based victims out of money or property, in violation of 18 U.S.C. § 1343, and then laundering those proceeds via the Binance cryptocurrency exchange, in violation of 18 U.S.C. § 1956(a)(1)(A). Enterprise #5's period of racketeering activity began no later than June 2021 and ended no earlier than November 2022 and involved dozens of violations of 18 U.S.C. § 1343 and dozens of violations of 18 U.S.C. § 1956(a)(1)(A)-(B) with respect to its victimization of Lenny alone. By knowingly allowing Binance to be used as a laundering facility and cash-out point for criminal syndicates that were engaged in a variety of international crimes, including wire fraud schemes to defraud Lenny and his co-Plaintiffs, Binance and Zhao tacitly conspired in Enterprise #5's pattern of racketeering activity.

C. The Proximate Causal Connection Between the RICO Enterprises' Racketeering and Plaintiffs' Economic Injuries

268. Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 267 above.

269. Defendants Binance, BAM, and Zhao's decisions that Binance would operate as an unregistered (and therefore unlawful) money transmitting business in violation of 18 U.S.C. § 1960(a), while Binance.US would serve as a smokescreen to divert United States regulators' and law enforcement's attention away from Binance, resulted in Binance's failure to comply with the Bank Secrecy Act's anti-money laundering requirements. That is, Binance knowingly and willfully used its lack of a FinCEN registration as a bogus explanation for why it did not need to comply with the Bank Secrecy Act's anti-money laundering requirements. Thus, there is a direct causal connection between Enterprise #1's, Enterprise #2's, and Enterprise #3's patterns of violations of 18 U.S.C. § 1960(a) and 18 U.S.C. § 1956(a)(1)(A)(i), on the one hand, and Binance's failure to comply with the Bank Secrecy Act's anti-money laundering requirements, on the other. And the FinCEN's investigation found that Binance's "willful failure to implement an effective [anti-money laundering] program," as required by the Bank Secrecy Act, "directly led to the [Binance] platform being used to process transactions" designed to "launder illicit proceeds" and "stolen funds." FinCEN also found that Binance's "willful failure to report to FinCEN hundreds of thousands of suspicious transactions inhibited law enforcement's ability to disrupt the illicit actors."

270. Accordingly, there is a proximate causal connection between Enterprise #1's, Enterprise #2's, Enterprise #3's patterns of racketeering activity—as well as Defendants Binance's, BAM's, and Zhao's participation in, directing, or conspiring with those enterprises' patterns of racketeering activity—and the Plaintiffs economic losses. In short, but for those RICO enterprises' racketeering activity and Defendants Binance's, BAM's, and Zhao's participation in, directing of, or conspiring with that racketeering activity, Binance would have registered with FinCEN as required by 18 U.S.C. § 1960(a) and operated with the anti-money laundering program

required by the Bank Secrecy Act, which would have thwarted fraudsters from using the Binance exchange to launder cryptocurrency that they stole from innocent victims, including Lenny and his co-Plaintiffs, and to convert that stolen cryptocurrency into fiat currency that United State law enforcement would never be able to recover and return to the victims.

271. But for Enterprise #4's and Enterprise #5's pattern of racketeering activity, the Plaintiffs would not have targeted and victimized by the pig butchering schemes in the first place. This is because it was the presence of the unlawful Binance exchange and the welcoming "cake" that it knowingly and purposefully offered to illicit actors that fueled the rise of the pig butchering schemes. At a minimum, however, but for Enterprise #4's and Enterprise #5's pattern of racketeering activity, the Plaintiffs would have been able to recover their stolen cryptocurrency assets with the assistance of United States law enforcement. This is because, but for Enterprise #4's and Enterprise #5's successful laundering and cashing out of the assets via the Binance exchange, the assets would have remained in the fraudsters' Binance accounts, easily traced through a forensic analysis of the blockchain, subject to rapid seizure by United States law enforcement, and available to be returned to the fraud victims. Binance and Zhao's participation in the conduct of Enterprise #4's affairs through violations of 18 U.S.C. § 1956 (a)(1)(A)-(B), and their conspiratorial assistance to and facilitation of Enterprise #5's violations of 18 U.S.C. § 1343 and 18 U.S.C. § 1956(a)(1)(A)-(B), were substantial factors in the fraudsters' ability to launder and cash out into fiat currency the cryptocurrency that they stole from the Plaintiffs, because the fraudsters needed Binance and its CEO Zhao to ignore and flout the applicable anti-money laundering laws, including "Know Your Customer" requirements and suspicious activity reporting obligations, for the fraudsters to use Binance successfully as a laundering facility and cash-out point. As the Department of Justice concluded from its criminal investigation of Zhao and

Binance, Zhao "knew and understood that his decisions with respect to Binance's AML program would likely have the result that Binance would facilitate . . . illicit transactions" on a massive, unprecedented scale.

272. With respect to proximate causation, what is true for Lenny is true for all of the Plaintiffs. Binance's systematic violations of federal criminal laws—laws that Congress designed and intended to ensure that financial institutions and financial platforms, including cryptocurrency exchanges, are free of money launderers whose underlying frauds prey on innocent Americans—facilitated and were a necessary ingredient to the success of the underlying frauds that inflicted devastating financial injuries on Lenny and his co-Plaintiffs. As alleged above, the Defendants knew and predicted that their systematic and willful violations of federal laws—which Binance's own employees described as offering a welcoming "cake" to criminals who otherwise would not be able to effectively launder their criminal proceeds—would lead to the very types of consequences that have ruined Lenny's and his co-Plaintiffs' financial wellbeing. As the United States put it in its April 23, 2024 sentencing memorandum in Zhao's criminal prosecution, Zhao's and Binance's conduct "expos[ed] our financial system and citizens to those who sought to exploit them, including criminal actors seeking a safe haven for the proceeds of their unlawful activity," and they "knew that Binance processed funds that were proceeds of unlawful activity or were used to promote unlawful activity." Zhao and Binance "The Defendants did not care, however, because by welcoming money launderers to the Binance exchange and concealing their crimes from United States regulators and law enforcement, the Defendants were making loads of money in transaction fees and thereby enriching themselves personally.

COUNT ONE
(Defendants Binance, BAM, and Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

273. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 272 above.

274. Binance, BAM, and Zhao were each associated with Enterprise #1 and participated in and/or directed the conduct of Enterprise #1's affairs through a pattern of racketeering activity, to wit, operating Binance in violation of 18 U.S.C. § 1960(a) (operating an unregistered and unlicensed money transmitting business) while seeking to deceive United States law enforcement and regulators about Binance's operations and conducting financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering).

275. The Plaintiffs were injured as a result of Enterprise #1's pattern of racketeering activity because, but for that racketeering activity, Binance would have registered with FinCEN and operated in compliance with the Bank Secrecy Act, such that the cryptocurrency assets that fraud operations stole from them would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to the Plaintiffs.

COUNT TWO
(Defendant Zhao)
(18 U.S.C. § 1964(c), for violations of 18 § U.S.C. 1962(c))

276. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 272 above.

277. Zhao was associated with Enterprise #2 and directed the conduct of Enterprise #2's affairs through a pattern of racketeering activity, to wit, directing the Binance exchange to be operated in violation of 18 U.S.C. § 1960(a) (operating an unregistered and unlicensed money

transmitting business) and to conduct financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering).

278. The Plaintiffs were injured as a result of Enterprise #2's pattern of racketeering activity and Zhao's direction of that activity, because, but for that racketeering activity and Zhao's direction it, Binance (1) would have registered with FinCEN and operated in compliance with the Bank Secrecy Act, such that the cryptocurrency assets that the fraud operations stole from the Plaintiffs would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to the Plaintiffs, and (2) would not have allowed or enabled the fraud operations to use Binance as a laundering facility and cash-out point for the cryptocurrency assets that the fraud operations stole from the Plaintiffs, but would instead have frozen the fraudsters' Binance accounts (*i.e.*, their Binance digital wallets), reported the suspicious transactions to FinCEN, and enabled United States law enforcement to recover the assets and return them to the Plaintiffs, or otherwise thwarted the fraud operations' conversion of stolen (but traceable, freezable, and seizable) cryptocurrency into untraceable and unrecoverable fiat currency.

COUNT THREE
(Defendant Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

279. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 272 above.

280. Zhao was associated with Enterprise #3 and directed the conduct of Enterprise #3's affairs through a pattern of racketeering activity, to wit, directing the Binance exchange to be operated in violation of 18 U.S.C. § 1960(a) (operating an unregistered and unlicensed money

transmitting business) and to conduct financial transactions on the Binance exchange in violation of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering).

281. The Plaintiffs were injured as a result of Zhao's directing Enterprise #3's pattern of racketeering activity because, but for that racketeering activity and Zhao's direction of it, Binance would have registered with FinCEN and operated in compliance with the Bank Secrecy Act, such that the cryptocurrency assets that the fraud operations stole from the Plaintiffs would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to the Plaintiffs.

COUNT FOUR
(Defendants Binance and Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(c))

282. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 272 above.

283. Binance and Zhao were each associated with Enterprise #4 and participated in the conduct of Enterprise #4's affairs through a pattern of racketeering activity, to wit, knowingly allowing financial transactions to occur on the Binance exchange that involved the proceeds of schemes to defraud United States citizens, with the intent to promote such fraudulent schemes and/or with the intent to conceal the nature and source of the proceeds, in violation of 18 U.S.C. § 1956(a)(1)(A)-(B) (engaging in money laundering transactions).

284. The Plaintiffs were injured as a result of Enterprise #4's pattern of racketeering activity because, but for that racketeering activity, the cryptocurrency assets that the fraud operations stole from the Plaintiffs would not have been laundered through and cashed out from Binance and instead would have been available to be seized by United States law enforcement and returned to the Plaintiffs.

COUNT FIVE
(Defendant BAM)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(d))

285. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 272 above.

286. BAM conspired with Enterprise #3's pattern of racketeering activity, to wit, Binance's operation of an unregistered money transmitting business in violation of 18 U.S.C. § 1960(a) and its concomitant violations of 18 U.S.C. § 1956(a)(1)(A)(i) (money laundering). BAM conspired with Enterprise #3's RICO violations by, among other things, agreeing to falsely represent to the public, United States regulatory agencies, and United law enforcement that all U.S.-based customers were being routed to the Binance.US exchange that had registered with FinCEN and was complying with the Bank Secrecy Act's anti-money laundering requirements, when BAM knew that Binance, at Zhao's direction, in fact continued to solicit, recruit, and retain U.S.-based market makers to provide the critical daily liquidity to the Binance exchange, in flagrant violation of 18 U.S.C. § 1960(a).

287. The Plaintiffs were injured by Enterprise #3's pattern of racketeering activity, as set forth *supra*. BAM's conspiratorial support of Enterprise #3's racketeering activity was a substantial factor in causing the Plaintiffs' injuries, because it substantially aided Binance's ability to fool United States regulators and United States law enforcement regarding Binance's obligation to comply with the Bank Secrecy Act's anti-money laundering requirements and, therefore, substantially aided Binance's ability to operate for as long as it did without the legally required anti-money laundering program that would have thwarted criminal organizations, such as and including the fraud operations that victimized the Plaintiffs, from using the Binance exchange as a laundering facility and cash-out point for their fraudulent schemes.

COUNT SIX
(Defendants Binance and Zhao)
(18 U.S.C. § 1964(c), for violations of 18 U.S.C. § 1962(d))

288. The Plaintiffs hereby reallege and incorporate by reference the allegations in paragraphs 1 through 272 above.

289. Enterprise #5 engaged in a pattern of racketeering activity, to wit, using international wire communications to defraud Lenny, his 25 co-Plaintiffs, and countless other American citizens of money or property, in violation of 18 U.S.C. § 1343, and then laundering those proceeds on the Binance cryptocurrency exchange to promote those fraud schemes and conceal the nature and source of the stolen assets, in violation of 18 U.S.C. § 1956(a)(1)(A)-(B).

290. Binance and Zhao conspired in Enterprise #5's pattern of racketeering activity, to wit, by allowing criminal syndicates including Enterprise #5 to use the Binance cryptocurrency exchange as a laundering facility and cash-out point for their illicit activities, either knowing or consciously avoiding learning that those transactions on the Binance cryptocurrency exchange involved the proceeds of illicit activity, promoted the success and continuation of such illicit activity, and concealed the nature and source of the stolen assets.

291. The Plaintiffs were injured as a result of Enterprise #5's pattern of racketeering activity because, but for that racketeering activity, the Plaintiffs would not have been defrauded at all or, at a minimum, would have been able to recover the cryptocurrency assets that were stolen from them. Binance's and Zhao's conspiratorial support of Enterprise #5's racketeering activity was a necessary component of Enterprise #5's ability to launder and cash out the cryptocurrency assets that Enterprise #5 stole from the Plaintiffs, which is what rendered the stolen cryptocurrency assets unrecoverable by the Plaintiffs and United States law enforcement.

PRAYER FOR RELIEF

WHEREFORE, each of the Plaintiffs pray for the following relief:

1. A treble damages award equal to three times the value of the cryptocurrency assets that the fraud operation stole from him or her and then laundered and cashed out through the Binance cryptocurrency exchange;
2. An order that Binance, Zhao, and BAM are jointly and severally liable for that treble damages award;
3. An award of statutory attorney's fees and costs; and
4. Any other relief that the court deems just and proper.

Respectfully submitted,

Dated: May 1, 2024

/s/ Aaron M. Katz

Aaron M. Katz
Keira Zirngibl
Patrick Dolan
AARON KATZ LAW LLC
399 Boylston Street, 6th Floor
Boston, MA 02116
(617) 915-6305
akatz@aaronkatzlaw.com
kzirngibl@aaronkatzlaw.com
pdolan@aaronkatzlaw.com

Eric Rosen
Constantine P. Economides (*pro hac vice* forthcoming)
Lance Aduba (*pro hac vice* forthcoming)
DYNAMIS LLP
225 Franklin Street, 26th Floor
Boston, MA 02110
(617) 802-9157
erosen@dynamisllp.com
ceconomides@dynamisllp.com
laduba@dynamisllp.com

Attorneys for Plaintiffs